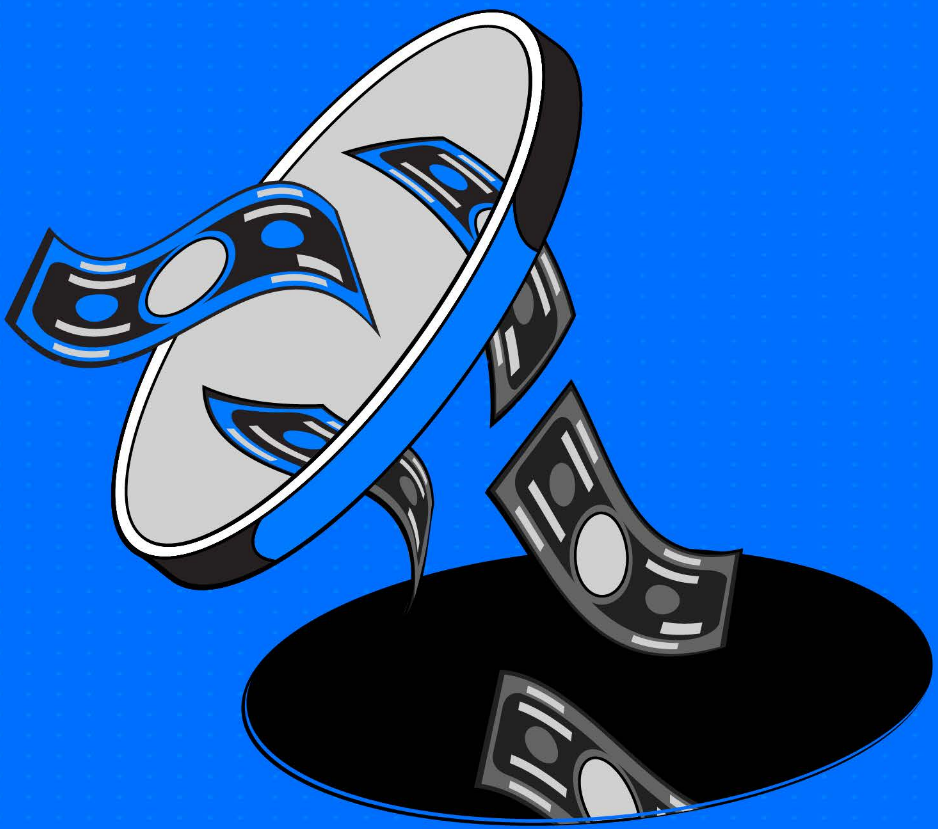
THE OTHER SIDE OF THE COIN

An Analysis of Financial and Economic Crime



EUROPEAN FINANCIAL AND ECONOMIC CRIME THREAT ASSESSMENT **2023**

EUROPEAN FINANCIAL AND ECONOMIC CRIME THREAT ASSESSMENT 2023

PDF | ISBN 978-92-95220-88-1 | ISSN 2811-8723 | DOI: 10.2813/105613 | QL-AX-23-001-EN-N

Photo credits:
© Nicolas Peeters: page 3.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: Europol (2023), European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

CONTENTS

FOREWORD

Catherine De Bolle
Executive Director
of Europol

I am pleased to present Europol's first European Financial and Economic Crime Threat Assessment. This is the latest flagship product in Europol's portfolio, a comprehensive and in-depth assessment of the threats posed by financial and economic crimes at EU level.

In our globalised world, trade, technology and transport bring us closer together and create economic opportunities and prosperity. However, there is another side to the coin; our interconnected world is misused and abused by criminal actors involved in economic and financial crimes. In fact, organised crime has built a parallel global criminal economic and financial system around money laundering, illicit financial transfers and corruption. Criminals exploit these three practices to conceal, move, and ultimately benefit from their criminal profits. The ability to launder illicit proceeds on an industrial scale, to move them through a web of criminal financial brokers, and to corrupt the relevant actors, has become indispensable for modern organised crime.

Criminal actors involved in economic and financial crimes capitalise on vulnerabilities in economic and social systems to generate billions in illicit profits. Meanwhile, with modern technology at their disposal, criminals have innovated and diversified their modi operandi in order to evade detection.

Thanks to the increasing efforts made by EU and national legislators, investigations into financial and economic crimes are growing in number and becoming more successful. Still, at present, the amount of assets that law enforcement manages to take away from the hands of criminal networks still remains below 2 % of the yearly estimated proceeds of organised crime, a drop in the ocean of the immense illicit – and untaxed – revenues gained by criminal networks. This is not something one police force or country can change by itself; we must strengthen existing cooperation and partnerships, and develop new approaches. Public-private partnerships in particular will play a pivotal role, as we can together prevent criminal profits from entering the legal financial system.

This is what led Europol to establish the European Financial and Economic Crime Centre (EFECC) in 2020. The main goal of this centre is to support national law enforcement authorities in their fight against financial and economic crimes, and to foster and support international cooperation and information exchange. Every year, the demand for Europol's support in asset recovery and financial investigations increases, and our skills and services are expanding.

This report presents findings of Europol's expert analysts in the world of financial and economic crime, detailing how the current threats are manifesting themselves and how these crimes impact wider society. Through this threat assessment, and our other analysis products, Europol wants to foster cooperation that will derail the world of criminal finances, intercept illicit profits, and – above all else – Make Europe Safer.

INTRODUCTION

Serious and organised crime continues to threaten the internal security of the EU. The criminal landscape constantly evolves, as criminals seek out new opportunities and exploit crises for their own interests. Criminal actors involved in economic and financial crimes are highly adept at taking advantage of our economy for their purposes, and at targeting increasing numbers of victims. They capitalise on vulnerabilities in society's systems to generate billions in illicit profits, while applying various strategies, often cyber-enabled, to remain undetected and secure their earnings.

Financial crimes, and in particular money laundering, undermine our society not only by infiltrating the legal economy, but also by fostering the growth of a parallel underground society made of individuals who increasingly rely on organised crime for their economic sustenance and livelihood. Vulnerable demographics, and especially vulnerable youngsters who are lacking trust in societal institutions and confidence in the rule of law, are the perfect target pool for such parallel underground society.

Due to their intrusive nature, financial and economic crimes are among the most challenging criminal activities to investigate and tackle. A fragmented landscape sees different criminal actors interact with one another, making criminal operations more complex and tangled. Key players typically remain anonymous and operate independently from established criminal structures, often from criminal safe havens. Meanwhile, their techniques and tools advance rapidly.

Some recent investigations, including those exploring encrypted communications among criminals, gave unprecedented insight into the system that sustains the finances of organised crime. While law enforcement is untangling the complexity of this underground financial ecosystem, information sharing, investigative focus on key criminal actors, development of technical knowledge and expertise, and public-private partnerships are essential tools for winning the fight against financial and economic crimes.

The European Financial and Economic Crime Threat Assessment describes the complexities of financial and economic crimes, and the criminal ecosystem that virtually sustains and links all other criminal activities. The report analyses all financial and economic crimes affecting the EU, such as money laundering, corruption, fraud, intellectual property crime, and commodity and currency counterfeiting. It also illustrates the power of asset recovery in the fight against financial and economic crimes.

The analytical findings of this report rely on a combination of operational insights and strategic intelligence contributed to Europol by EU Member States and Europol's partners, who provided crucial information regarding the criminals' business models. The report is intended to capture the pervasiveness and destructiveness of financial and economic crimes affecting the EU, and to support all relevant stakeholders in untangling the large variety of financial and economic crimes.

THE DRIVERS OF TODAY'S FINANCIAL AND ECONOMIC CRIMES

Financial and economic crimes continue to evolve, driven by a series of developments in the broader environment such as technological acceleration and digitalisation, and global and regional geopolitical crises. However they are also influenced by the evolution of serious and organised crime; adept in exploiting opportunities, criminal actors involved in financial and economic crimes display new expertise, target more victims than ever, and put further distance between themselves and their criminal activities.

Serious and organised crime as a driver

As the criminal landscape in the EU keeps on changing and evolving, so does the complex spectrum of financial and economic crimes. Criminal actors take advantage of the vulnerabilities of our system, weakening our society in the process, while generating enormous profits. As serious and organised crime thrives, criminals involved in financial and economic crimes also evolve, as they need to be able to launder illicit proceeds and manage an underground criminal financial system capable of sustaining the wealth of other criminal actors. They also need to build bridges to relevant actors with access to power or information in crucial sectors of society and business, for which corruption is key. Therefore, money laundering, criminal finances and corruption continue to constitute the main engines of the organised crime machine[1].

The digital acceleration

The COVID-19 pandemic led to an unprecedented shift towards online services, so that normal activities could continue remotely despite restrictions on movement of people and goods. Existing digital services were expanded and many others moved online. An extensive remote working regime was introduced in many business sectors, including staff performing critical and sensitive tasks. With consumers increasingly looking online for goods and services, offenders quickly adapted their modi operandi to the digital environment[2], abusing weakened IT protocols, setting up fake investment websites, trading in illicit and counterfeit goods, and targeting e-commerce businesses, in particular for fraud.

The digital acceleration of society led to a significant increase in cyber-enabled financial and economic crimes. Financial crime performed through the use of computer technology is particularly attractive to criminals, as it helps to obscure money flows and allows faster and greater profits. The cyber component offers serious and organised crime a greater pool of targets to victimise multiple times. At the same time it leads criminals to develop technologies facilitating, on one hand, the anonymity of the perpetrators, and on the other hand, collaboration among criminals. Encrypted messaging apps, dark web marketplaces, cryptocurrencies, and other privacy-enhancing technologies protect their identity, making law enforcement detection increasingly challenging. Besides, illicit digital products and technical services can also be hired or purchased by criminals in a crime-as-a-service business model, allowing criminals who are not particularly tech-savvy to perform illicit activities that entail knowledge of technology.

Rapid technological advances in the financial sector have been taken on by criminals as opportunities. Fintech (a portmanteau of 'financial technology') integrates technology to improve financial services, which drives innovation, expands financial inclusion and reduces operational costs. Fintech is now integrated into traditional banking, but also in non-bank and non-financial organisations. Yet, it provides many opportunities for criminal abuse.

Other developments in finance have led to the arrival of digital banking, or neo banks, which are virtual financial institutions with no physical branches. Such banks are increasingly popular, often growing quickly and at the expense of proper compliance processes, which risks disproportionate rates of financial fraud and money laundering offences. In this context, the use of digital payments for money laundering purposes has been observed in all Member States, and this practice appears to be growing at varying rates[3]. Virtual IBANs[I] (vIBANs) enable fast international payments that mask the identity of the master account, the issuer and country of origin, making it harder to detect suspicious transactions, and adding an extra step to investigations. The misuse of vIBANs has been observed in recent criminal investigations into various fraud types.

Buy now pay later (BNPL) financing, also known as point-of-sale instalment loans, has also grown recently[4] and criminals have been exploiting current weaknesses in the BNPL application process for theft. Since BNPL services do not conduct formal credit checks, offenders can often pass the algorithmic checks and use legitimate users' accounts to illicitly order items. Machine learning, artificial intelligence (AI) and deepfake technology can be used for virtually all types of financial and economic crime. Chat-bots based on AI, such as ChatGPT, could be easily used in online fraud schemes[5]. Deepfake technology can help circumventing remote on-boarding measures. CEO fraud is a particular risk, as information on high-profile figures at financial institutions is publicly available.

Decentralised finance (DeFi)[II] involves using blockchain technology to supplement or replace the traditional centralised financial system. The decentralised blockchain technology promises greater independence and security, as sensitive information can be protected more robustly. However, the lack of regulation of this new area leaves openings for economic crime, since criminals hold illicit assets on DeFi platforms. The use of cryptocurrencies for criminal schemes is also increasing in line with their overall adoption rate[6] (however their criminal use still represents less than one percent of the overall transaction volume)[7]. Offenders appear to be deterred by their high volatility and by some high-profile law enforcement successes in tracing criminal cryptocurrency transactions. However, cryptocurrencies are still largely targeted in fraudulent investment schemes and are also used for a wide range of criminal activities, ranging from trade of illicit goods to fraud and money laundering. Non-fungible tokens (NFTs) are unique digital identifiers that are recorded in a blockchain. They have grown

[I] Virtual IBANs are IBANs issued by a bank to allow rerouting of incoming bank transfers to a master account, to help distinguish between multiple payees. They are functionally identical to conventional IBANs and can be used to send and receive payments. They are also composed of up to 34 alphanumeric characters. The key difference between regular and virtual IBANs lies in account matching. A regular IBAN is linked to only one single physical bank account. By contrast, a virtual IBAN is a virtual number that is not matched to an account in a physical bank. They are bank-issued reference numbers that enable incoming payments to be rerouted to a physical IBAN, which is itself linked to a physical bank account. They cannot hold any funds, and their balance is constantly zero.
[II] Technologies that do not rely on third parties to facilitate the exchange, loan and payment of cryptocurrency.

significantly in popularity in recent years, and many cryptocurrency exchanges now offer NFTs directly on their platforms. NFTs are frequently abused for fraud: fake NFTs are sold by criminals and legitimate ones are sold multiple times. NFTs also pose a significant risk of money laundering, due to their instant trading feature across borders.

The metaverse is a set of open and interoperable digital spaces which can be used for many aspects of daily life. The financial sector has been an early adopter, and many actors have established a presence in the metaverse. Criminals will certainly exploit it further as this new virtual environment develops, with cases of fraud, theft, and other crimes already being reported[8]. The current research into new decentralised web platforms and applications based on peer-to-peer (P2P) interaction rather than on centralised data hosting services could be exploited by organised crime and constitute a further challenge for investigations[9].

Geopolitical developments

As the EU continues to engage with its partners globally, political developments happening around the world are impacting the EU's external and internal security landscape. China, through a series of economic investments globally and in the EU, continues to exert political influence at global level. China's Belt and Road initiative is reshaping the EU freight transport system, while, in line with the global trend, state-owned Chinese companies are increasing their control of several major EU sea terminals.

At the periphery of the EU, active conflicts continue to threaten regional stability and may cause further mass migration movements towards the EU. This fuels not only the migrant-smuggling industry that has emerged over recent years, but also the rise of other forms of crime which benefit from vulnerable demographics and economic uncertainty.

In 2022, the Russian war of aggression against Ukraine and the related spikes in prices and rising inflation have caused economic hardship for many, while opening greater opportunities for criminal actors. Disruptions in global supply chains and in provisions of services opened up opportunities for frauds and diversion, while an increase in the cost of living provided chances to criminals to exploit vulnerable individuals and businesses in economic distress.

SANCTIONS EVASION AND ITS LINKS TO ORGANISED CRIME

Since March 2014, the EU and the wider international community have progressively imposed a broad range of measures on Russian organisations and individuals, including financial measures, trade sanctions, travel bans, and asset freezing. The objective of these measures is to weaken Russia's economic base by depriving it of critical technologies and markets, and by limiting its capabilities for war[10].

Depending on the type of sanction imposed, targets of EU sanctions have used a variety of illicit mechanisms to circumvent them. Methods used include concealment of beneficial ownership, use of intermediaries and fraudulent documents, and the relocation and undervaluation of movable assets. The use of third countries to channel transactions from Russia is a common element. Information available has reflected links and similarities with money laundering modi operandi[11], including potential involvement of specialised money laundering networks that may act as service providers for sanctioned individuals.

Over the past year, there have been reports of individuals detected in EU countries or attempting to enter the EU[12] from Ukraine in possession of significant amounts of cash (in some cases millions of euros). Although the origin of the money could not be established, it is suspected that some of the individuals may have acted as money mules for third parties attempting to launder illicit funds or, potentially, to evade EU sanctions[13]. The EU has also prohibited the sale, supply, transfer, and export of euro-denominated banknotes to Russia, aiming to limit access to euros by Russian entities to help prevent circumvention of sanctions[14]. Furthermore, there have been numerous instances of Russian-speaking individuals attempting to smuggle large amounts of euros in cash from the EU to Russia, which are suspected of being connected with Russian-speaking crime syndicates[15]. In addition to cash transactions, cryptocurrencies are also likely to be used in money laundering schemes related to evasion of sanctions.

Case example

In January 2023, law enforcement authorities took down a crypto-platform suspected of being used by criminals to launder illicit funds belonging to Russian entities under EU sanctions. Bitzlato allowed the rapid conversion of various crypto-assets such as bitcoin, ethereum, litecoin, bitcoin cash, dash, dogecoin, and tether into Russian rubles. It is estimated that the crypto exchange platform has received assets worth a total of EUR 2.1 billion (BTC 119 000). While conversion of crypto-assets into fiat currencies is not illegal, investigations into the cybercriminal operators indicated that large volumes of criminal assets passed through the platform. Analysis indicated that about 46 % of the assets exchanged through Bitzlato, worth around EUR 1 billion, were linked to criminal activities[16].

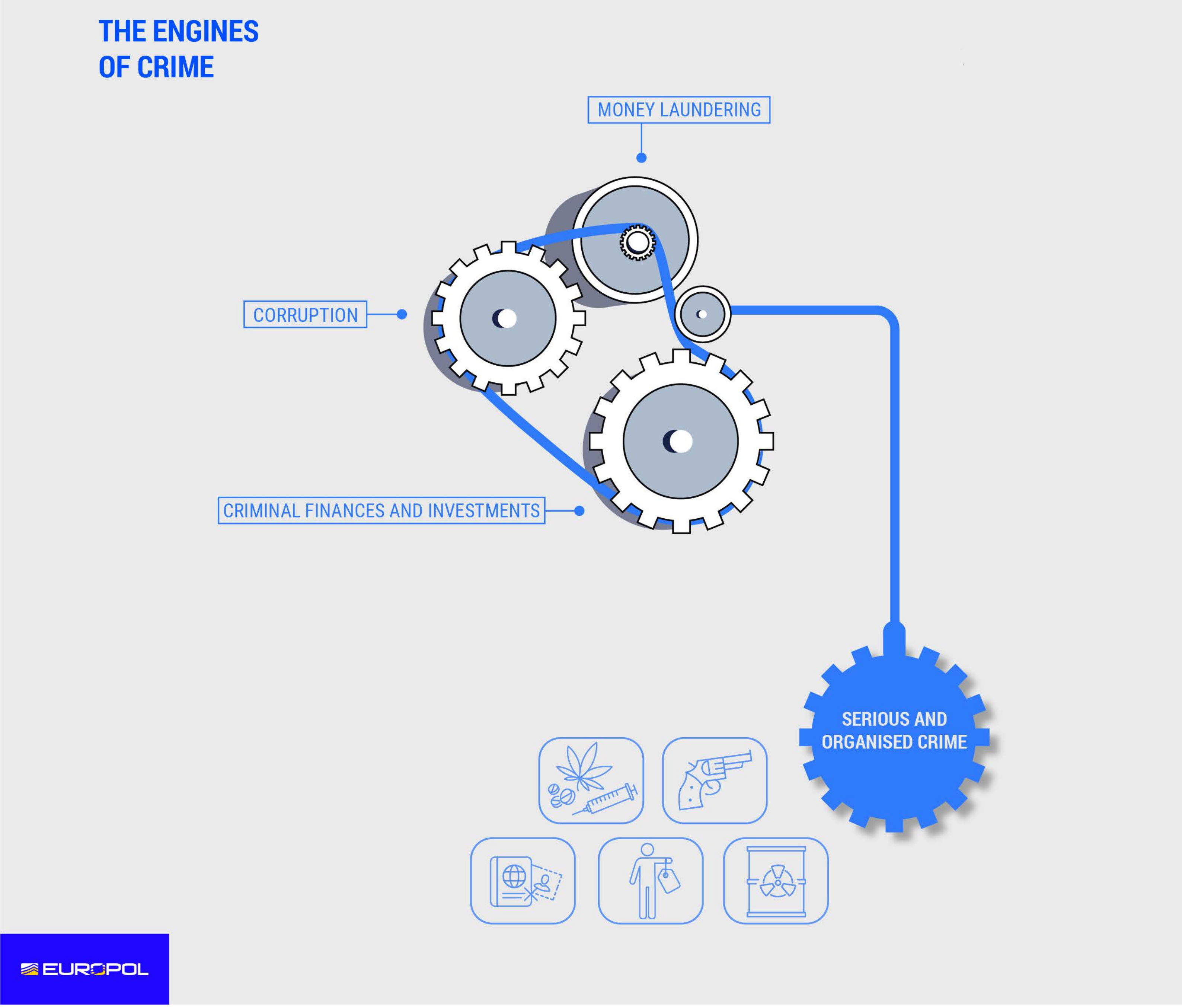
MONEY LAUNDERING, CRIMINAL FINANCES AND CORRUPTION; THE ENGINES OF CRIME

For the machine of serious and organised crime to function and thrive, three main components need to operate at full speed. Firstly, the capability to launder industrial levels of illicit profits. Secondly, a sophisticated financial crime ecosystem that allows for criminal business continuity. Thirdly, an ever-expanding web of corruptors and corrupted, enabling criminals to have access to information and power.

Money laundering, criminal finances and corruption are as pervasive and disruptive for society as they are indispensable for criminal actors. Almost 70 % of criminal networks operating in the EU make use of basic money laundering techniques, while 60 % use corruptive methods to achieve their illicit objectives[17]. Their far-reaching tentacles corrode the rule of law, grind down people's trust in the justice system and its institutions, and weaken societal and economic growth. The lines between the illicit and licit world become increasingly blurred; criminal finances and investments are tangled with licit ones.

Due to their intrusive yet imperceptible nature, these criminal activities are also among the most difficult to investigate and tackle. Key players often remain anonymous and are coordinating and controlling their activities from outside the EU, while their techniques and tools advance promptly.

Infiltration into the legal system is what makes crime pervasive and destructive. More than 80 % of the criminal networks active in the EU misuse legal business structures (LBSs) for their criminal activities[18]. The abuse of LBSs is even more essential for criminal networks involved in economic and financial crimes. Due to the nature of their criminal activities, which constantly bridge between the licit and illicit economy, the façade of a legitimate business is key for evading law enforcement attention. To facilitate their operations, criminals own or infiltrate commercial entities. Trading companies, online service providers, IT enterprises, call centres, investment firms, delivery and shipping services, and logistical suppliers are all used for criminal operations, and also for exploiting the weaknesses in national tax regimes and concealing the links between the members of fraudulent schemes. Front or shell companies are largely used by money laundering syndicates. Cash-intensive businesses are also often targeted, as they provide opportunities to mix licit and illicit proceeds. Complex systems of corporate entities are spread across multiple jurisdictions and sometimes include offshore branches.



Money laundering: a global, collaborative crime

Money laundering is the process by which criminals conceal the illegal origin of their property or income[19]. In a simplified representation of a more complex reality, the process can be divided into three main stages. The first stage involves the placement of the illicit profits into a legitimate financial system. The second stage is the layering, which involves a series of conversions or movements of the funds to distance them from their source. The third stage is the integration, when the laundered profits re-enter the legitimate economy, through investments into real estate, luxury assets, or business ventures[20]. The digitalisation of the economy is slowly but steadily reshaping the known money laundering process, making the various steps of the procedure much more blurred. The ever-growing use of digital transactions is resulting in the placement phase being less frequent, as illicit profits (e.g. gained in digital currencies) are in fact already circulating within the legal financial system. This makes the layering phase more crucial for the obfuscation of the flows. Meanwhile, the proliferation of money laundering as-a-service has rendered the process fragmented across different criminal groups.

Money laundering generally takes place following a predicate offence, but can also be performed by criminals as their main activity[21]. While part of the illicit proceeds are reinvested to cover past and future operational costs, clean money accrues in the hands of the criminal leaders, and is used to pay the network members and facilitators. Enabled by globalisation, which has brought with it financial transactions without borders, international banking, and digital finance, money launderers quickly move illicit funds collected in the EU to anywhere in the world. Complex transaction chains, involving different jurisdictions, make it very difficult for the financial investigators to follow the money trail and freeze or recover funds.

- Money laundering is a pivotal activity for the full spectrum of serious and organised crime, enabled by globalisation and the digitalisation of the financial sector. Almost 70 % of criminal networks operating in the EU make use of basic money laundering techniques, and about 30 % engage with professional money laundering networks and/or underground banking system.

- Money laundering is performed through informal value transfer systems (IVTSs), cash smuggling, transfer of funds, trade-based money laundering (TBML), digital asset trading and/or investments in the legal economy. An ever-growing list of digital assets is used to launder proceeds from both online and offline crimes.

- The abuse of legal business structures (LBSs) is key in money laundering; licit and illicit funds can be easily mixed, and the identity of beneficial owners is masked by layers of corporate structures spread across multiple jurisdictions, often offshore.

- Professional money launderers have established a parallel underground financial system to process transactions and payments away from surveillance mechanisms governing the legal financial system. Some high-level money brokers hold a central position in the criminal ecosystem. Offering wide-ranging unregulated and worldwide banking and escrow services to multiple criminal organisations, they have links to the upper echelons of organised crime.

Every year, serious and organised criminal networks operating in the EU launder billions of illicit profits, making money laundering a key criminal threat for our societies.

Money laundering is performed in different ways, either by members of the criminal network involved in a predicate offence, or by professional money launderers and money brokers. In the first case, the way in which the illegal proceeds are cleaned differs according to the predicate offence, the amount of money, the frequency of the operations and of illicit profits, and the geographical location of the members. In the second instance, the launderer or money broker chooses the most suitable way to launder the money, often according to the amount, but also to their own business capabilities and available assets.

Money laundering as-a-service

Almost 70 % of criminal networks operating in the EU make use of basic money laundering techniques, while the rest engage with professional money laundering networks and/or make use of an underground banking system[22].

The crime-as-a-service business model is prevalent in money laundering. Professional money launderers have established a parallel underground financial system to process transactions and payments away from surveillance mechanisms governing the legal financial system[23]. Professional money launderers are both individual entrepreneurs as well as networks, and offer their services for a fee often to multiple criminal networks at the same time. They may hold financial information on criminal funds (cash, bank accounts, crypto wallets, legal business structures etc.) and probably some information on the identity of their clients, but no information about their criminal business. These service providers offer up-to-date expertise, while distancing the criminal network from the illicit funds. They use the whole spectrum of laundering tools and techniques, handling the entire process from on-site cash collections to timely and global delivery of cleaned assets in any form. Their commission-based fee is 5-20 % of the laundered sum, and varies based on the geographical origin and destination of the funds.

Money laundering criminal networks consist of both EU and non-EU nationals. The non-EU criminals mainly originate from Eastern Europe, the Middle East, Asia and Africa. Among these, Chinese money laundering networks operate cash collectors and couriers throughout the EU, and misuse legitimate transport companies to transport cash concealed among goods or in hidden compartments of cars. Smurfing techniques[III] are applied for bank transfers. Chinese money laundering network controllers also operate using more sophisticated methods, for example as money brokers offering insurance and accountability for international transfers. They set up contracts between the parties and they are able to transfer value from one country to another without physical movement of cash. Money is transformed into other commodities and compensation schemes, and combining IVTSs and TBML. The magnitude of EU-China trade allows them to obfuscate the illicit money flows[24].

The business model of the money broker

Some high-level money brokers are able to run a parallel underground financial system. They are known also as money laundering network controllers[25], because of their central position in the criminal landscape, and as they are the single contact point for the criminal clients. They offer wide-ranging unregulated and worldwide banking services to multiple criminal organisations.

Some brokers are well-known and trusted, while others work through personal references. They offer collection for a pick-up and remittance for a drop-off of cash, and facilitate transactions between third parties offering escrow services. They offer insurance and accountability through guarantees of the transferred values. The broker oversees a network of permanent or freelance regional coordinators, who run the daily business in relevant jurisdictions. This allows the broker to offer services globally and respond swiftly to the needs of clients. Local coordinators confirm the existence of criminal money in the EU and send instructions to the broker located in jurisdictions outside the EU to recognise the value there. Both sides confirm the exchange with the use of tokens. The regional coordinator also manages a network of cash collectors or cash runners. Once the cash is collected, the token is given to the client (e.g. drug dealer) as a proof of the handover and an insurance that the cash will be remitted

[III] A money laundering method used to split illicit proceeds into smaller sums before placing these small amounts into the financial system to avoid suspicious transaction reporting.

according to the conditions agreed between the parties. In order to deliver the cleaned assets back to the criminal network, the broker may use any of the relevant money laundering techniques.

The money broker is central in this business model as the sole contact point with the client and the sole holder of key information on amounts transferred and methods used. They keep detailed records of their customers in different jurisdictions and regularly reset their accounts, keeping a regular balance of financial flows. This means funds can be paid in and out with minimal movement of actual fiat currency.

Companies located in offshore jurisdictions play a key role in money laundering schemes involving organised crime. Money brokers are established mainly outside the EU, and they usually rely on large networks of international business partners and LBSs. They also rely on close and long-lasting partnerships with networks active in EU Member States, allowing them to deploy cash collectors to different locations simultaneously.

Case example

A high-value target belonging to a large criminal network was arrested because of his involvement in money laundering for other criminal networks. The suspect was a regional coordinator in charge of several cash collectors based in Spain. They were involved in underground banking activities for several criminal organisations there, working under a broker operating from Dubai. The coordinator used cars equipped with concealed compartments to collect and transport cash, following instructions from the network controller in Dubai. Using this structure, they laundered up to EUR 15 million per month, and over EUR 200 million over the investigation period. An action day in September 2022, headed by Spain, led to the arrest of 6 suspects and 14 searches, as well as the seizure of EUR 500 000 cash, 2 properties, 7 vehicles equipped with hidden compartments, several bank accounts, documents, and numerous digital devices[26].

Money laundering methods and typologies

Money launderers use a variety of methods and techniques to obscure the source of illicit profits and mask the identity of the final beneficiaries of the funds reintroduced into the legal economy. The methods and typologies can be applied in one or more stages of placement, layering and integration.

Informal value transfer systems – underground banking

An informal value transfer system (IVTS) is any system, mechanism, or network of people that receives money to make the funds or an equivalent value payable to a third party in another geographic location[27], operating outside the regulatory oversight of the legitimate banking sector. It is also referred to as underground banking. The implementation of stricter anti-money laundering regulations in mainstream financial institutions has made IVTSs increasingly attractive to criminals and criminal networks. IVTSs are commonly used to move the proceeds of migrant smuggling, organised property crime, trafficking in human beings, and drug trafficking[28]. Hawala[IV] is a type of IVTS used to move and launder illicitly gained proceeds of crime. Hawaladars (those

[IV] Also known as fei qian (fei ch'ien, 飞钱) in China, or black market Peso exchange in South America that operate Hawala) often run separate parallel businesses, particularly currency exchanges, travel agencies, or telephone shops.

Cash smuggling

When illicit proceeds are moved physically around the globe, cash is sent in consignments or packages, or transferred by cash couriers[29]. Couriers may be recruited by criminal networks and managed by regional coordinators, in many cases they are financially vulnerable people who accept the risky business in exchange for money. Cash is temporarily stored in caches, and is then transported by various means, including passenger and freight transport, by road, and air transport. Transportation generally takes a few days and is mainly done during weekends[30].

Regular large-scale cash seizures from cash couriers throughout the EU indicate that cash smuggling is still widespread. Cash is transported within the EU or to/from non-EU countries. Cash amounts seized at land borders are generally larger, while seizures at EU airports are more frequent. Restriction in air traffic from Ukraine affected cash seizures at airports involving cash transfers to or from Russia. Cash smugglers switched to land routes in response, using trucks and cars to cross the external borders of the EU into Eastern European countries[31].

Mule networks exploit the banking system

Money mules are individuals who, often unknowingly, have been recruited as money laundering intermediaries for criminals. They transfer illicit funds between accounts, often in different countries, on behalf of others[32], using personal and/or corporate bank accounts.

Money mules are often part of a larger money laundering scheme, adding layers of distance between operations, goods or victims, and criminals. Like cash couriers, money mules mainly offer their service for a fee instead of being involved in the predicate offence. Money mule accounts are sometimes opened through impersonation or identity theft[33]. Investigations reveal recruitment of students, migrants, and vulnerable people in financial need. Mules are recruited intensively through social media, particularly in fraud schemes. Money mule coordinators recruit and manage the money-mule network, so to keep them far from the criminal leaders.

Trade-based money laundering (TBML)

Criminal networks are increasingly involved in TBML, a method that exploits foreign trade and transit procedures to move criminal funds using false invoicing and documentation. Criminals set up trading structures operating with goods and services across many sectors and jurisdictions. The most commonly traded goods include second hand vehicles, metals, clothes, construction equipment, medical devices, fish products, real estate, watches, high value goods, gold, clothing, art (artefacts, antiques, non-fungible tokens (NFTs))[34] and even horses[35].

TBML entails multiple stages: proceeds of crime are transformed into commercial products, taking on an air of legitimacy, before being brought into the financial sector without attracting the attention of law enforcement. TBML can also serve as an illicit money remittance system through trade misinvoicing schemes: merchandise is purchased legitimately, then a misinvoicing scheme is applied. When these schemes are used to convert illicit proceeds into international commercial products, it then becomes a case of TBML[36].

Third-party intermediaries are a common feature of TBML schemes, often featuring in the invoice settlement process. TBML requires a large amount of cash up front to buy goods to trade. Criminal networks involved in highly profitable criminal activities, such as drug trafficking, are able to finance it. It can be combined with value-added tax (VAT) fraud, including carousel fraud. *Daigou* (surrogate shopping) is a type of TBML involving the use of illicit proceeds to internationally buy luxury goods which are then put for sale in China, taking advantage of higher retail prices.

Digital assets

Criminal synergies are growing between online and offline spaces[37], and professional money laundering service providers have started to offer cryptocurrency as-a-service[38] for both online and offline crimes, for instance for fraud, cyber-attacks, drug trafficking, racketeering, and VAT fraud (including carousel fraud), often offering services on dark web marketplaces.

Advances in investigation techniques have helped detect suspicious transactions and identify actors. Many EU Member States have seen illicit funds channelled to cryptocurrency trading platforms and police have seized codes for crypto accounts, cards, or applications on cryptocurrency exchanges as proceeds of crime. Yet the global nature, speed, and mixing of cryptocurrency transactions present a significant challenge to law enforcement investigations. It is also difficult to trace and freeze crypto assets, and convert them into fiat currency. Therefore, criminals have partly shifted to DeFi[V], cryptocurrency mixers, NFTs, peer-to-peer marketplaces, and more privacy-oriented cryptocurrencies, e.g. privacy coins. Criminals have also been using stable coins, in order to avoid fluctuations in the value of cryptocurrencies; they have started to use them not only to move value, but also to store value in wallets out of reach of law enforcement.

Cryptocurrency exchanges play a key role[39], facilitating exchanges between fiat and cryptocurrency. During the placement stage, money brokers open several accounts using money mules and false identity documents, and receive cash from criminals to be exchanged for cryptocurrencies. Brokers sometimes contact private vendors located in different EU countries to purchase cryptocurrencies with cash or other coins. Not all providers of virtual currency services comply with adequate due diligence measures to identify and monitor business relationships, and complicit cryptocurrency service providers offer the exchange of virtual currencies for cash for a commission[40]. During the layering stage, illicit funds are separated from their original source by exchanging the primary coins for other coins. In this process, also known as “chain hopping”, money is moved from one cryptocurrency to another, across poorly regulated exchanges and jurisdictions, to create a money trail that is difficult to track. The layering process may involve cryptocurrency mixers (or tumblers), which break the links between the original and the final address using several intermediary wallets, charging a transaction fee. Finally, the new cryptocurrency appears “clean”. In the integration stage, often money mules are used to open several bank accounts in one or more countries, which remain open for a short period of time for quick transfer of funds from the cryptocurrency wallets. Alternatively, criminals create online companies to accept payments in cryptocurrency. Some criminals opt to keep the laundered funds in the form of another coin rather than convert it into fiat currency[41].

Other cryptocurrency services are also used for money laundering. Crypto ATMs are a form of exchange used to convert fiat currency into cryptocurrency and vice versa, to launder criminal proceeds and to transfer funds overseas. NFTs allow specific individual items to be sold and traded on a blockchain. Another popular obfuscation technique is channelling criminal proceeds into cryptocurrency gambling platforms, where criminals can claim to have gambling wins. These platforms are often hosted in

[V] Decentralised Finance (“DeFi”) is another important element in the cryptocurrency market. Decentralised exchanges allow for users with unhosted wallets to transact without a centralised party that is obliged to conduct KYC and AML, leading to a further loosening of standards. Whereas traditional exchanges are focussed on turning fiat currencies into cryptocurrencies, decentralised exchanges are focussed on turning cryptocurrencies into other coins and currencies.

non-EU jurisdictions and internal transactions are hard to trace. Crypto vouchers[VI] and prepaid debit cards are used as payment methods.

The misuse of legal business structures: from restaurants to banks

Cash-intensive businesses are easily misused for money laundering as they provide ample opportunities to mix licit and illicit proceeds. A large volume of small transactions, the use of high denominations, and the variety of regulations for the use of cash payments across the EU[VII] are all factors that criminals can exploit. Bars, restaurants, pizzerias, grocery shops, construction companies, motor vehicle retailers, car washes, art and antique dealers, auction houses, pawnshops, jewellers, textile retail, liquor and tobacco stores, retail/night shops, gambling services, strip clubs, and massage parlours are common examples of the cash-intensive businesses criminals may use for laundering purposes.

Licit money service businesses are misused to move criminal cash internationally[42]. The funds are channelled through complex payment chains with many intermediaries across multiple jurisdictions. Money-transfer services are extensively used for laundering funds from trafficking in human beings, migrant smuggling and cybercrime[43]. Multiple layers of shell companies set up in various jurisdictions, sometimes offshore[44], are regularly used for money laundering. Such companies often have no commercial activity and are set up to conceal the ultimate beneficial owner (UBO)[VIII] or the illicit source of the funds. Shares in shell companies may also be passed on to transfer ownership[45]. Offshore professionals provide clients with shell companies and with trusts containing corporations, holdings, and shareholding stakes, in order to conceal ownership and create a veneer of legitimacy[46]. Company bank accounts are registered in the name of non-resident entities or proxy persons (strawmen)[47], usually for a fee. Strawmen may be associated with multiple legal entities. Legal advisers help in the setting up of the shell companies and open bank accounts. In order to deposit cash in bank accounts or transfer funds through money service businesses, money laundering networks usually use smurfing techniques.

Case example

The Pandora Papers, made public in 2021, comprise almost 12 million leaked documents exposing hidden wealth, tax avoidance, and money laundering by prominent individuals and politically exposed persons. They show how international networks for illicit finance enable criminals to launder criminal proceeds, hide assets, engage in corruption, and sustain a globalised criminal economy. The papers reveal complex international networks of companies, often using offshore locations, to hide ownership of money and assets[48].

[VI] Crypto vouchers work like prepaid cards and offer the possibility to instantly redeem a voucher code for a wide range of crypto currencies.
[VII] According to the Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, an EU-wide maximum limit of EUR 10 000 is set for cash payments. Member States will have the flexibility to impose a lower maximum limit if they wish. The Sixth Anti-Money Laundering Directive has been approved by the Council and the Parliament and should become fully operational in 2024. Full text accessible at https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf
[VIII] The Ultimate Beneficial Owner (UBO) is the natural person who ultimately owns or controls the company and/or the natural person on whose behalf a transaction is conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Investment of criminal assets in the legal economy

Criminal networks invest in high-value movable goods (luxury cars, jewellery and other luxury items), real estate, precious metals, cash-intensive businesses, the gaming sector, holdings and charity funds, digital assets, and in the criminal business itself. Illicit proceeds are sometimes laundered through football clubs. Criminals may appear as sponsors, or manipulate matches so their teams can participate in sponsored tournaments[49]. Clubs may be purchased by front men for companies registered in offshore jurisdictions and high-risk countries for money laundering. Cross-border transactions justified as player payments/transfer fees or television rights may conceal illicit money flows (see also section on fraud schemes linked to sporting events). Criminal networks continue to convert illicit cash into gold as it offers anonymity, it secures value, and it can be safely stored and transported, then sold anywhere over the counter. Money laundering involving gold may be detected when transfers made to gold source countries are quickly withdrawn in cash.

ASSET RECOVERY

Asset recovery is a powerful deterrent and an effective tool to tackle serious and organised crime[50]. It deprives criminals of their ill-gotten assets and prevents them from reinvesting them in further crime or integrating them into the mainstream economy.

The asset recovery process includes several phases:

- tracing and identification of tainted assets;
- seizing the assets with a view to possible subsequent confiscation;
- management of seized assets until a final decision is made;
- confiscation of the tainted assets;
- disposal of the confiscated assets, which could include their reuse for public or social purposes.

Freezing assets involves ‘temporarily prohibiting the transfer, conversion, disposition or movement of assets or temporarily assuming custody or control of assets on the basis of an order issued by a court or other competent authority’[51], meaning that the owner cannot dispose of their assets before a case is closed. Seizure instead means to temporarily restrain an asset or put it into the custody of the government and may apply to physical assets (i.e. a vehicle), also pending the outcome of the case. Confiscation is a final measure designed to stop criminals from accessing property obtained illicitly. Such property is taken away permanently from the criminal or their accomplices[52].

Regulation (EU) 2018/1805 is the current legislation covering freezing and confiscation orders in the EU. Its main features are the establishment of a single regulation covering both freezing and confiscation orders that are directly applicable in the EU, as well as recognition and enforcement of judicial decisions made in one EU country in another. It imposes a 45-day deadline for the recognition of a confiscation order and, in urgent cases, a 48-hour deadline for recognition with another 48 hours allowed for execution. Victims’ rights to compensation and restitution are also ensured under this regulation. A new EU Commission proposal for a Directive in 2022[53] addresses asset recovery from beginning to end; this Directive is expected to enhance asset recovery and asset management, partly through asset management offices (AMOs) in all Member States. The proposal also makes it possible to sell a frozen asset before it is confiscated. EU Member States will have to set up registries with information on frozen and confiscated assets, and collect statistics to measure progress in tackling illicit proceeds.

ESTIMATING SEIZURES AND CONFISCATIONS OF ASSETS

The amount of seized and confiscated assets is a useful performance indicator to assess the effectiveness of the asset recovery instrument in the fight against serious and organised crime. However, EU-wide endorsed statistics on the amounts of seized assets remain unavailable, despite growing efforts being made to synchronise the collection, recording and management of such assets.

For this report, an ad hoc data collection on seized assets was carried out with support from the contributing Member States. These estimations, even if conservative, aim to put the revenues produced by serious and organised crime and the amount of criminal assets being successfully recovered into perspective. Based on information received from 24 EU Member States, the value of seized assets in the EU annually amounted to at least EUR 4.1 billion on average in 2020 and 2021. Thanks to the growing law enforcement focus on recovery, the value of estimated seizures has almost doubled, compared to a previous estimate done in 2016: from EUR 2.4 billion on average per year for 2010-2014, up to 4.1 billion on average per year in 2020 and 2021[54]. Cash was the most commonly seized item, followed by bank accounts and vehicles. Less frequent categories of assets seized include shares, gold, other movable property (including vessels), and virtual assets[55].

There is currently no fully reliable data available on illicit proceeds generated by serious and organised crime in the EU. Therefore we need to be very cautious in formulating estimates of the share of illicit proceeds seized. An overall conclusion may however be that the large majority of illicit proceeds remain in the hands of organised crime. When taking into consideration the revenues of organised crime, the most recent approximations on yearly profits of nine criminal markets in the EU ranged between EUR 92 to 188 billion[56]. Therefore the seized criminal funds would amount to 4.4 % to 2.2 % of the total illicit revenues. Considering that even the larger estimate of EUR 188 billion is undoubtedly an underestimation of the real profits of serious and organised crime (as for just one large-scale EU operation, the seized criminal funds alone amounted to almost EUR 900 million[57]), the amount of assets that law enforcement manages to take away from the hands of criminal networks still remains below 2 % of the yearly proceeds of organised crime.

Increasing efforts are being made by EU legislators, Member States and law enforcement to corrode the economic power of serious and organised crime through the recovery of confiscated assets. Yet the amount of captured proceeds still represents just a drop in the ocean of the immense illicit – and untaxed – revenues gained by criminal networks.

CRIMINAL ASSETS IDENTIFIED OUTSIDE THE EU

Professional money laundering networks offer their services globally to deliver criminal proceeds to those in charge of the predicate offences. Investigations have shown that money is often destined for or invested in the countries where criminals live. It remains particularly hard to confiscate assets in third countries, especially in uncooperative jurisdictions, and criminal networks also capitalise on such challenges.

Digital assets, and their increasing use, represent another big challenge in seizures and subsequent management. Most countries do not yet have the experience and the specialist expertise required for tracing, analysis of the blockchain, clarification of actual ownership, management of the assets seized, time of sale, and recovery. Digital assets held in non-financial institutions are even more difficult to trace, seize, and confiscate.

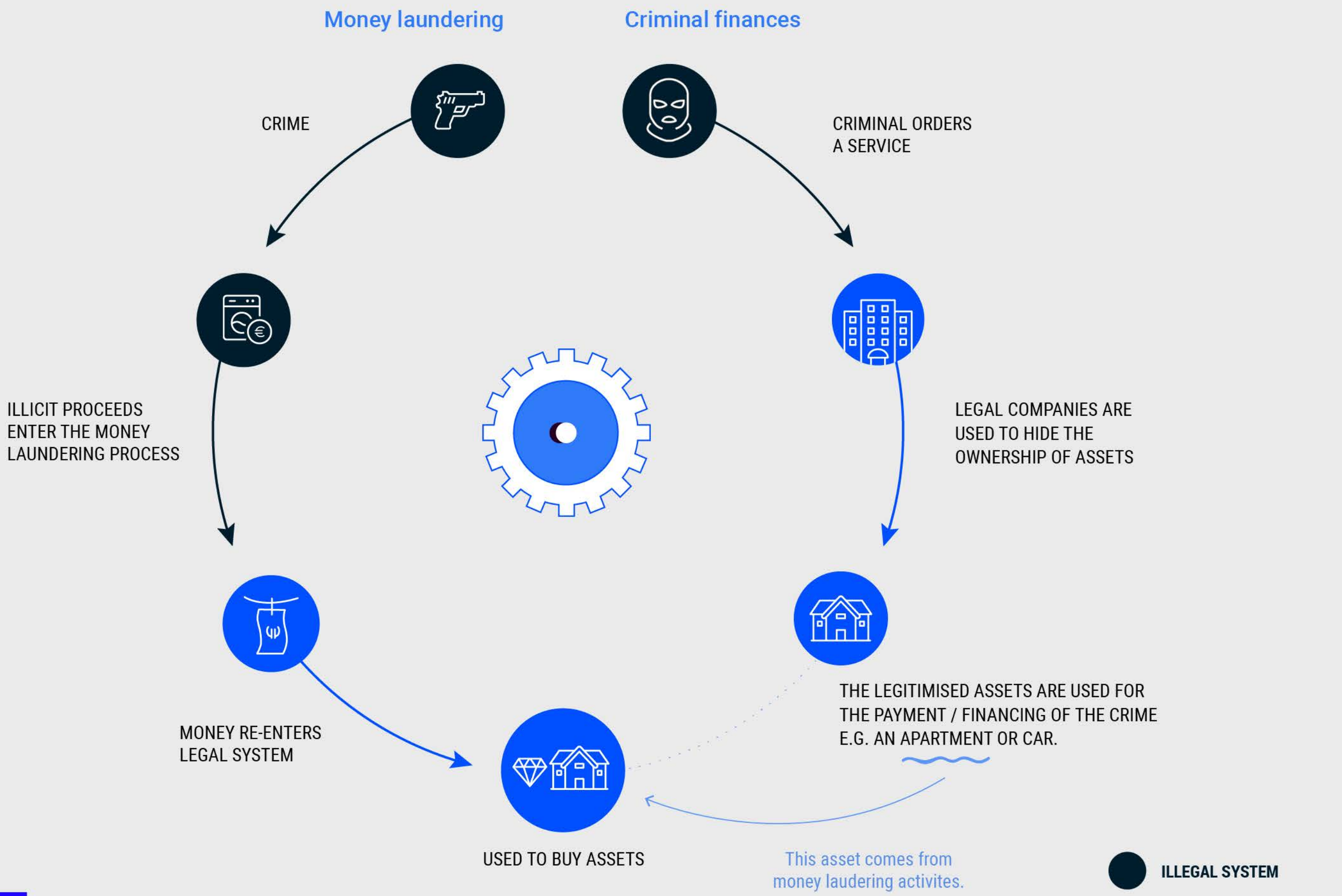
The asset recovery process includes several steps that involve different competent authorities. Their cooperation is key, especially that of the asset recovery offices (AROs) and the AMOs, but also with any stakeholder handling information that can assist in asset tracing.

Criminal finances and investments

Enhanced EU legislation in the field of anti-money laundering, and the resulting increase in financial supervision in the banking sector, have made it more difficult for criminal networks to introduce illicit proceeds into the legal economy through traditional banking channels[58]. Against this backdrop, criminals continue to explore alternative methods for managing assets originating from illicit activities while avoiding detection. For this purpose, criminal proceeds are invested in and intermingled with the legal economy, i.e. real estate, food service industry, cash-intensive businesses, company shares etc. This development accelerates in times of economic crisis and has the potential to undermine the legal economy.

As well as the variety of methods and typologies that professional money launderers apply for these ends, some criminal actors have established a system of criminal finances[59]. Criminal finances are assets in whatever form and format that derive from previous criminal activities and are already successfully laundered and integrated into the legal economy. Criminal finances are used to foster further criminal activity by means of investment or payment and help to root criminal networks into the legal economy and society.

CRIMINAL FINANCES AND INVESTMENTS



Profits derived from years of intense criminal activities - and already laundered into physical and financial assets - are being lawfully administered by a series of private companies and by financial and other experts[60]. In some cases, these actors are unaware of the criminal origin of the assets. When needed, the ownership of these assets is exchanged between companies, either as a means for payments and/or as an investment. The fact that there are no financial transactions involved during the transferral of assets makes it challenging for investigators to link the movement of assets to a criminal venture.

Investment into organised crime promises high yields and criminal investors use their illicitly accumulated and therefore unexplained wealth to finance criminal activities, like the importation of illicit goods to the EU by local criminal networks.

Corruption

Corruption is the abuse of entrusted power for private gain[61]. It trades power or relevant information in exchange for cash, goods, services or privileges. It occurs at all levels of society and targets individuals in both public and private sectors. Corruption is an insidious and often invisible threat, eroding the rule of law, weakening state institutions, and hindering economic development by distorting fair competition. Corruption affects decision-making, reduces the availability and quality of public services, redirects investments against the public interest, and distorts normal business dynamics. It has an impact on all segments of modern society and weakens citizens' trust in democracy, creating a negative perception of national and international institutions.

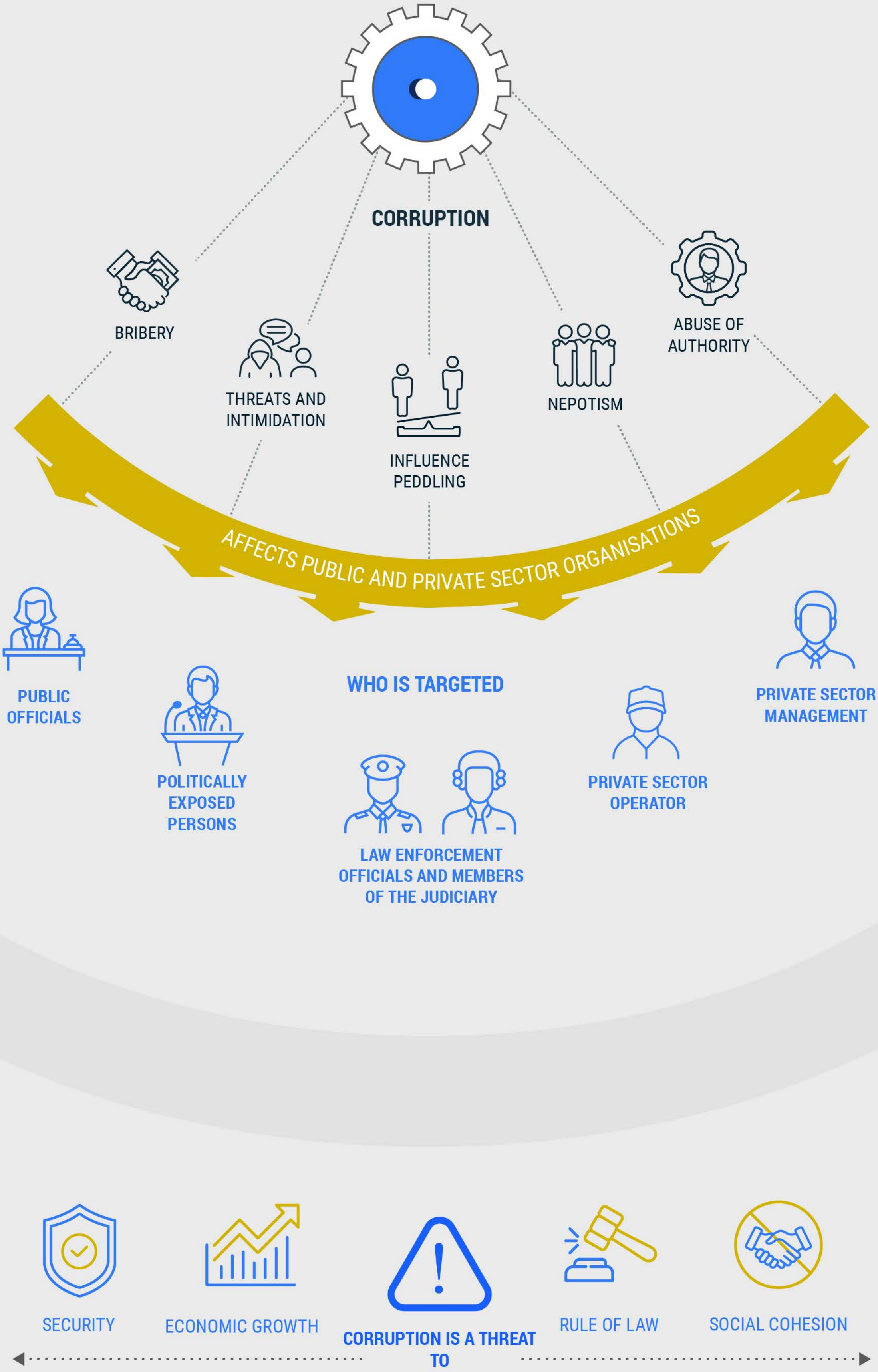
- Corruption is an indispensable instrument for organised crime. It is a key enabler of most criminal operations, yet for some actors it is a prerequisite for their crimes' success. 60 % of the criminal networks operating in the EU use corruptive methods to achieve their illicit objectives.

- The costs of corruption remain marginal in the economy of organised crime. Bribery varies according to the situation; in some cases bribes reach hundreds of thousands of euros. The huge profits of organised crime enable criminal networks to pay high bribes to facilitate further crime.

- Networks of corrupted individuals operate in multiple organisations and geographic locations. In some cases, corruption is facilitated by independent brokers acting as service providers.

Individuals are targeted for corruption either because of their position of power or because they hold relevant information. Targets of corruption usually work in critical sectors and generally have no criminal background or previous convictions. Corrupted people range from low-ranking employees or officials to high-level representatives in both the private and the public sectors, including political figures at local, national and international levels. People entrusted with public functions in public administration and law enforcement, as well as prosecutors and judges, are particularly attractive targets for corruption.

THE TOOLS AND TARGETS OF CORRUPTION



Corruption and serious and organised crime

As corruption may happen at all levels of society, it is an indispensable instrument for organised crime. Corruption is globally widespread along all smuggling routes. Through corruption, organised crime takes hold of local, regional and national administrations, business entities, and key logistical and transportation hubs.

Criminal networks need multiple points of access to organise the basic operations of their criminal business and to protect them against interventions by law enforcement and judicial authorities. Considering corruption as one of the marginal costs of their business, criminal actors build networks of corrupted individuals across multiple organisations and hubs to facilitate their operations and obstruct investigations. Corruption is used in all steps of criminal activities; corrupted associates in different countries are used for coordinating and enabling the trafficking chain at entry, transit and exit hubs. For example, criminal networks engage in corruption to control critical infrastructure such as ports, to ensure that incoming cocaine shipments are successfully received by criminal customers. Police officials, customs officers, security staff, and other personnel at sensitive transportation hubs and at border control points are approached to provide information and ensure trafficked goods can pass unimpaired. Corrupted law enforcement and justice officials also provide sensitive information and influence investigations[62].

Some criminal networks may build networks of corrupted individuals in multiple organisations and hubs, often via multiple channels. In some cases, corruption is facilitated by independent brokers acting as service providers[63]. The highest bribes are paid to essential links in the extraction chain, often crane operators, planners or employees providing access to information via IT systems. Coordinators of extraction teams receive between 7 to 15 % of the value of the illicit load[64]. Corruption is sometimes combined with intimidation and threats, or debt bondage, coercion and blackmail, particularly when those corrupted want to end the cooperation[65].

Corruption and money laundering are tightly interwoven. This is also true for large-scale corruption, which involves practices such as large payments to bank accounts and offshore companies across different jurisdictions, the use of complex corporate schemes to obfuscate the real beneficiaries, making investments in property or in a country's economy, and luxury items offered as gifts. Corruption involves millions of euros of illicit funds, and corrupted entities use professional criminal networks to help launder the bribes they receive.

Criminals obscure the source and ownership of funds in corruption schemes, so people receiving bribes can hide their illicit funds and thus make it difficult to detect when corruption is taking place[66]. Money laundering investigations are therefore key to revealing corruption schemes. A financial intelligence report or suspicious transactions report from a financial investigation unit (FIU) often leads to a criminal investigation for corruption. These investigations follow money through tangled corporate networks that link to entities and people that may be either known criminal actors or high-level officials with assets that are not justified by their legitimate activities.

Key typologies and modi operandi

Corruption mainly takes the form of bribery (both giving and receiving a bribe) with the aim to secure services and influence decisions. Bribes can be cash payments, deposits in bank accounts, gifts (goods or services), election grants, paid holidays, transfers of real estate, or use of luxury cars. Bribes might be paid directly to the corrupted person or given to close relatives or associates. Influence peddling (also known as trading in influence, or abuse of office or functions) is also a common means of corruption, which entails using one's influence in government or connections with persons in authority to obtain favours or preferential treatment for another actor, usually in return for payment.

Corruption can manifest at every stage of tender: in the preparation of tender specifications, in the tender application, during the selection and evaluation of proposals, and when awarding the tender. A public official could be convinced to accept a proposal from a specific bidder, inhibiting fair competition and the application of public procurement rules. The official might also leak confidential information regarding the tender procedure or the other applications. Another example would be that the official ensures that control activities, audits, checks, or inspections do not identify any potential irregularity in relation to the project proposal[67]. Influence peddling may involve restricting procurement contracts to a limited group of actors who illegally eliminate competitiveness.

Sectors in continuous expansion, such as the construction and sustainable energy sectors, are increasingly being targeted for influence peddling and corruption in tendering procedures. Organised crime often operates hiding behind a complex network of corporate entities and sub-contracting companies. Criminal actors colluding with public officials to determine the winner of a bidding process is called bid rigging. Healthcare was the most severely affected sector during the COVID-19 pandemic; urgent procurement needs created opportunities for subsidy fraud, favouritism, and misappropriation of funds. In certain cases, criminal networks owned the companies participating in bid-rigging processes, and bribed officials during the procurement process. A new form of corruption arose in connection with the pandemic, with public employees being bribed to issue vaccination certificates[68].

Lobbying for unlawful influence is another tool of corruption. Officials or politicians, at all levels, unlawfully lobby to influence decisions and procedures in return for money or other benefits. Corruption practices also include nepotism, extortion, and influence on witnesses.

THE WORLD OF FRAUDS

Criminal actors involved in fraud schemes include both opportunistic individuals and criminal networks. They differ according to the type of fraud, their level of expertise, the targets chosen, and the tools and techniques that they use. Nowadays, most frauds are cyber-enabled. Fraud schemes cause a significant amount of harm, both financial and otherwise, as they affect individuals, the public and private sector, as well as the financial interests of the EU and the Member States.

Fraud schemes against individuals, public and private sectors

Fraud offences use deceit for voluntary but unlawful transfer of money, goods, or undue advantages. Fraud schemes with a wide range of targets are present in all Member States but under-reported, as victims seek to protect their name and reputation[69].

- The criminal actors engaged in fraud schemes span from opportunistic individuals to highly organised networks, with mid-level management layers and external criminal service providers with expertise in tax, banking, law, finance, IT, and money laundering. As a multitude of frauds nowadays are cyber-enabled, fraudsters are avid customers of cybercrime as-a-service, making use of tools and/or data on offer.
- Fraudsters either target large pools of potential victims or victimise selected targets. Re-victimisation of targets is a common practice. Social engineering and impersonation are the most used techniques.
- The most common types of fraud include investment frauds (especially crypto-investments), business email compromise (BEC), e-commerce frauds, tech support frauds, romance frauds and phishing campaigns.

Criminal networks operating frauds rely on technical knowledge and external criminal service providers with relevant expertise to help commit the crime. Fraudsters are knowledgeable about their targets, and use facilitators such as call centre operators, money mules and cash couriers. Both EU and non-EU criminal networks engage in fraudulent schemes, frequently targeting victims speaking the same language but located far away, often across multiple countries. Money mules and money launderers are often located in other countries than the fraudsters.

Fraudulent schemes are increasingly run online, using digital tools and techniques, although some types of fraud traditionally include face-to-face interaction between fraudsters and victims. Fraudsters increasingly use sophisticated and varied social engineering techniques to target potential victims—often based on their status, psychological conditions and habits, as extensive information can be found online. Impersonation is one of the main tools used in online frauds. Fraudsters impersonate bank officials, CEOs, legitimate businesses and vendors, IT officers, police officers, relatives and acquaintances of victims.

Fraudsters quickly adapt to exploit current socio-political trends and international crises. The COVID-19 pandemic in 2020 and the expedited shift to the online environment for people and businesses opened up many opportunities to fraudsters, who were offering fake goods and services and bogus investments[70]. Following the outbreak of the Russian war of aggression against Ukraine in 2022, fraudsters targeted victims across the EU under the guise of supporting Ukraine or Ukrainians. Fake webpages were set up and fake emails were sent from fraudulent addresses, sometimes impersonating genuine celebrity campaigners. Fraudsters also targeted Ukrainians via instant messaging services for social benefit fraud using their personal information, offering subsidies via fake government portals[71].

Investment fraud

Investment fraud is a key threat in the EU, causing substantial losses for individuals and companies. The number of online investment fraud investigations reported to Europol has increased over the past two years but victims remain reluctant to report the crime[72].

Offenders are constantly refining their modi operandi[73]. Investment fraud schemes traditionally relying on face-to-face interaction have moved online, including Ponzi schemes, pyramid fraud schemes, and advance fee fraud. Fraudsters commonly seek out victims on social media platforms, but also use e-mail, instant messaging applications, or dedicated investment websites. Online advertisements invite victims to open online trading portfolios and lure them in with initial benefits. When a victim asks for explanations of why they cannot withdraw their money, the criminals fake legitimate reasons, and encourage the victim to pay more money for their funds to be released[74].

Most cases of investment fraud in the EU involve cryptocurrencies. Other types of fraudulent investments concern forex, real estate, precious metals, the energy sector, offshore holdings, stock exchange markets, binary options, non-existent virtual currencies, and pension funds. Perpetrators adapt to socio-economic trends and shift their focus on attractive new products (such as initial public offerings[IX] or venture capital investments[X]) and exploit opportunities linked to political developments (carbon credits, legal cannabis, and oil prices)[75].

After carrying out the fraud, criminals often contact victims pretending to be lawyers or law enforcement agents offering help in exchange for a fee. Some investment fraud schemes have integrated COVID-19 restrictions into their narratives as a justification for not returning profits or investments[76]. When the cryptocurrency market saw a sharp decline in 2022, a parallel decline in the revenues from crypto scams was detected[77]. If the decline in the cryptocurrency market continues, cryptocurrencies might become a less attractive investment product, and therefore criminals carrying out this type of fraud may focus elsewhere.

[IX] The Initial Public Offering (IPO) process occurs when a previously unlisted company sells new or existing securities and offers them to the public for the first time. Prior to an IPO, a company is considered to be private. After an IPO, the issuing company becomes a publicly listed company on a recognised stock exchange.
[X] Venture capital is a form of private equity and a type of financing that investors provide to startup companies and small businesses that are believed to have long-term growth potential. Venture capital generally comes from well-off investors, investment banks, and any other financial institutions.

Investment fraud involving cryptocurrencies is increasingly linked to other types of fraud, such as romance scams, meaning re-victimisation. A dangerous combination of a romance scam and investment fraud sees criminals slowly building a relationship of trust with the victim and then convincing them to invest their savings on fraudulent cryptocurrency trading platforms, leading to large financial losses. Liquidity mining is another type of fraud that also involves victims' grooming, as fraudsters often target crypto holders interested in liquidity mining - a DeFi process in which crypto holders lend their crypto assets to a decentralised exchange to obtain passive income from trading fees accrued from traders swapping tokens.

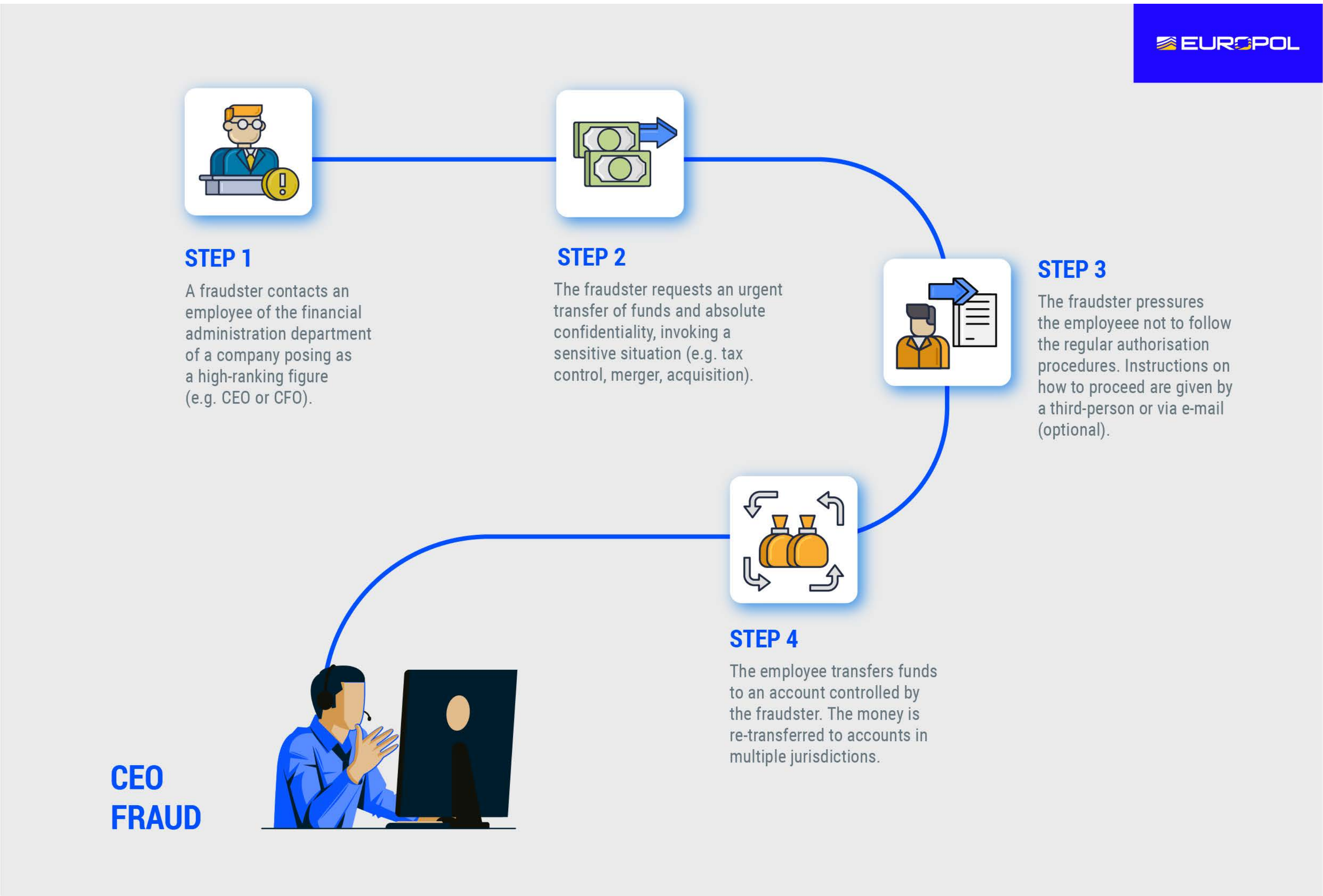
Case example

A criminal network used the social media platform 'Vitae.co' and the website 'Vitaetoken.io' to trick people into investing in a cryptocurrency Ponzi scheme. Around 223 000 individuals from 177 countries are believed to have fallen victim to it. The members of this criminal network included Belgian nationals who used a company under Swiss jurisdiction. Over EUR 1 million in cash was seized, along with EUR 1.5 million in cryptocurrencies and 17 luxury vehicles[78].

Business e-mail compromise (BEC)

Also called payment diversion fraud, BEC is a highly profitable fraud targeting EU private businesses and organisations that often operate internationally, perform wire transfers and have networks of suppliers. Chief executive officer (CEO) and fake invoice frauds represent the most common BEC categories[79], particularly effective due to the combination of social engineering and sense of urgency transmitted to the victims. Criminals either hack the victims' email or send messages to the targets that appear to come from within the organisation (usually a financial department, a manager or an employee) or from a business partner, making a request for a quick transaction with some sort of imperative justification (as an acquisition or a tax control, or the change of banking details), or asking to pay an invoice that looks genuine - but with the recipient's account modified by the scammers. Victims who follow the instructions may be wiring several transfers before realising that it is a scam.

Social engineering plays a key role, as fraudsters use publicly available information about employees, direct collaborators, and business partners, among other things, to sound convincing. Phishing is often used to obtain personal and security data, enabling fraudsters to access and manipulate communication. BEC is often linked to subsequent investment and non-delivery frauds (when it involves fake invoices). Fake invoice fraud through impersonation often targets intellectual property (IP) owners throughout the application process, with fraudsters posing as competent IP offices[80].



E-commerce fraud

E-commerce fraud, a substantial and growing cause of economic damage over the last two years, encompasses non-delivery fraud, card-not-present fraud, first-party fraud, art scams, accommodation fraud, fake ticket fraud, fake shipping fees, and fake custom fees. Fraud related to NFTs is also emerging[81]. First-party fraud types (including non-payment, overpayment, and chargeback fraud) are growing, causing financial damage to merchants globally.

E-commerce fraud sometimes starts with mass-mailing phishing, and it often involves re-victimisation. Fraudsters reach potential victims by abusing legitimate web shops and by creating similar fake ones for triangle fraud (the practice of selling fake cheap products, stealing customer credit card data, and ordering the goods from the genuine shop), causing financial loss and reputational risk to legitimate vendors. Criminal networks increasingly revert to phishing and social engineering[82]. As authentication mechanisms have been strengthened, fraudsters can less frequently commit fraud using solely credit card details. Therefore they increasingly access accounts through account takeover (ATO) in order to perpetrate fraud. Some criminal networks use phishing kits sold online by cybercriminals.

Case example

A criminal network composed of nationals from different African countries residing in the EU set up a sophisticated fraud scheme combining BEC and e-commerce fraud. The fraudsters faked email addresses and websites to impersonate legitimate wholesale companies and receive orders from other companies, mainly European and Asian. Advance payments were requested and the goods were never sent. Proceeds were laundered through Romanian bank accounts controlled by the criminals, then withdrawn at ATMs[83].

Tech support fraud

Also called helpdesk fraud, tech support fraud is an emerging type of fraud targeting EU citizens and employees of banking institutions. Using social engineering and IT tools, scammers contact their victims, posing as the IT helpdesk or anti-fraud departments of banks and other established tech organisations, usually via a spoofed phone number or a pop-up message sent to the victim's device. They claim there is a technical problem with their computer or bank account, and offer assistance through access to the victim's devices and security details. This lets the scammers install a remote access Trojan or malware. Once holding login details, scammers make money transfers, often to foreign bank accounts handled by money mules.

Romance fraud

Romance fraud heavily relies on information collected via open sources, and requires few technical IT skills. It mainly begins on social media and dating apps. Fraudsters often impersonate real individuals living in countries hit by conflicts or remote locations, using pictures found on open sources. The modus operandi involves gradually gaining victims' trust, then getting closer. Once victims are hooked, scammers start eliciting personal and financial information, or making urgent requests for money using a range of pretexts, such as the need to buy airplane tickets, gift cards, advance payments for shipping packages, medical expenses, car repairs, loans, travel documents, visas, etc. Scammers usually ask for money transfers to third countries, or via a gift card or prepaid card.

This type of fraud may last months or even years, generating substantial illicit profits. After romance fraud, fraudsters often target the same victims with other fraud schemes (e.g. investment and e-commerce fraud) or even induce them to commit frauds on their behalf. Victims are often abused as money mules, for e-commerce frauds, and for money laundering, but also for sextortion and identity theft.

Recovery or refund scam

Recovery or refund scam is often consequent of an earlier fraudulent scheme, usually e-commerce, tech-support or investment fraud. Perpetrators, either the same offenders or their associates, approach scammed victims and offer them help to retrieve back their money or goods. In both cases, perpetrators ask for advance fees to open a refund request/case.

Mass mailing

Mass-mailing fraud schemes are perpetrated mainly via email, but also via social media and post. Fraudsters impersonate known business or government entities to request money transfers with fake promises of rewards. Mass mailings are mostly untargeted, using large-scale phishing campaigns, with a small proportion of individuals eventually falling prey. Once payments from victims are processed, fraudsters withdraw the money and disappear. Mass mailing is commonly linked to schemes focusing on foreign lotteries, 419 scams[XI], credit and loan scams, mass blackmailing, fake competitions and investments, public authority impersonation, and charity scams.

Case example

In an online scam in 2022, fake correspondence was sent via email and social media, purportedly from Europol departments and senior staff. The message told victims that they had visited websites hosting child sexual abuse material, and urged them to reply to an email address. Respondents were asked to make a payment between EUR 3 000 and 7 000 via bank transfer or instant money services to avoid prosecution[84].

Food fraud

Fraud involving food presents important hazards for public health, but is attractive for criminal actors due to the potentially high profit margins. Food or drinks in a poor state of conservation or expired/spoiled are relabelled and reintroduced into the supply chain. In some cases, waste disposal centres are compliant in this criminal business, selling the food to the criminal actors rather than proceeding with its destruction (for which they had already received payment).

Other types of food fraud involve the illegal use of protected designation of origin and protected geographical indications, or the fraudulent attribution of the organic category for standard products, misleading the consumer.

Case example

A two-part investigation across several EU Member States has unveiled a criminal network involved in food fraud. In 2023, 27 suspects were arrested for relabelling millions of expired food products and reintroducing them into the supply chain. They acquired immense quantities of expired food and beverages and would chemically erase the expiry date and reprint a new one, or forge new labels. The suspects are believed to have made at least EUR 1 million in profits[85].

[XI] Also referred to as the 'Nigerian scam'. In the 419 scam the fraudster tricks the victim into paying money under the promise of a future, larger payoff. Victims are asked to help them to transfer funds out of their country in return for a share of the money. Sometimes they are asked bank account information and up-front payments.

Fraud schemes against the financial interests of the EU and Member States

Criminal actors operate several types of fraudulent schemes that have a detrimental impact on the financial interest of one or more Member States, and of the EU as a whole. Billions of euros are defrauded every year from State and Union budgets via subsidy frauds, excise frauds (tobacco, energy fuel and alcohol), custom import frauds, and VAT and carousel fraud schemes.

- VAT (including carousel) fraud generates several billions of euros and will remain a highly lucrative area for criminal networks.
- Production of counterfeit tobacco products in the EU has increased. Criminal networks involved in the smuggling and production of illicit tobacco products are resilient.
- Subsidy fraudsters will continue to target EU funds supporting sectors such as renewable energy, research programmes, and agriculture.

Subsidy fraud

Subsidy or grant fraud includes plagiarism, selling the same piece of research to different entities, participation in tender applications based on false declarations, submission of false progress reports, and provision of fictitious invoices. Subsidy fraud typically involves embezzlement, double funding, and the manipulation of justifying documents. It requires knowledge of subsidy application processes and can be facilitated by corruption. With the EU focusing on a more sustainable, digital, and resilient economy, subsidy fraudsters are set to increasingly target sectors such as renewable energy, research programmes, and the agricultural sectors - some of the 'pillars' of the EU Next Generation Fund (NGEU)[XII].

[XII] The EU recovery plan, NextGenerationEU (NGEU), is a unique funding mechanism, unprecedented in scope, intended to ensure the EU's recovery from the COVID-19 pandemic and to build a greener, more digital, and more resilient EU. Worth EUR 806.9 billion, it operates from 2021 to 2023 and is based on the provisions set out in the national Resilience and Recovery Plans (RRPs) for each Member State. Subsidy fraud and corruption are key threats to NGEU awarding and spending, as criminal actors target recovery funds. Fraudsters may bribe key officials (including auditors and evaluators) to ensure that their project is awarded a NGEU grant or loan, or so that correct implementation is inaccurately recorded and funds are disbursed. Double funding and conflict of interest are also emerging vulnerabilities. Criminals and criminal networks may implement corrupt practices throughout the funds allocation cycle: application, implementation, and closure and evaluation. Investigations need to target all levels. NGEU will provide significant additional financial resources to be used in a limited timeframe, which may lead to simplified procedures or emergency procurement processes that present a significantly higher risk of abuse. European Commission, 2021, The EU's 2021-2027 long-term Budget and NextGenerationEU, Facts and Figures, accessible at https://op.europa.eu/en/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-en

Case example

In October 2021, Europol launched operation SENTINEL to counter criminal activities threatening the NextGenerationEU recovery fund, particularly fraud, corruption, embezzlement, misappropriation and money laundering. Irregularities and crimes are investigated by the 21 EU Member States participating, either under their national competences or by the European Public Prosecutor's Office (EPPO), Eurojust and the European Anti-Fraud Office (OLAF), in accordance with their respective legal frameworks[86].

Social benefit fraud, a sub-category of subsidy fraud, is committed when an individual or a company obtains state benefits that they are not entitled to, or deliberately fails to report a change in their personal circumstances that would make them ineligible to receive such benefit. This fraud takes various forms, and cases have involved COVID-19 financial support schemes. Besides the common link with document fraud and money laundering, social benefit frauds may also relate to other crimes, such as migrant smuggling or human trafficking for labour exploitation.

Case example

In June 2021, the French National Gendarmerie and the Israeli Police hit a criminal network running a sophisticated benefit fraud scheme. This criminal syndicate is believed to have swindled the French State out of EUR 12 million in COVID-19 unemployment benefits by using 3 600 shell companies. Fraudulent proceeds were paid into French bank accounts, then immediately moved across Europe. French authorities raided several addresses to arrest accomplices – all were family members. A total of EUR 1 765 630 and USD 3 420 in cash was discovered, together with luxury watches and jewellery. The French authorities also recovered over EUR 6.2 million from bank accounts. The Israeli Police took action against the members of this same criminal group located in Israel, arresting an accomplice and searching a call centre believed to have been used to organise these large-scale scams[87].

Excise fraud

Goods such as alcohol, cigarettes, and fuel are subject to excise duty upon production in or on import into the EU[XIII]. Excise duties are indirect taxes on the sale and use of specific products, and countries that apply high excise and VAT rates are more vulnerable to sale of illicit excise products.

Tobacco

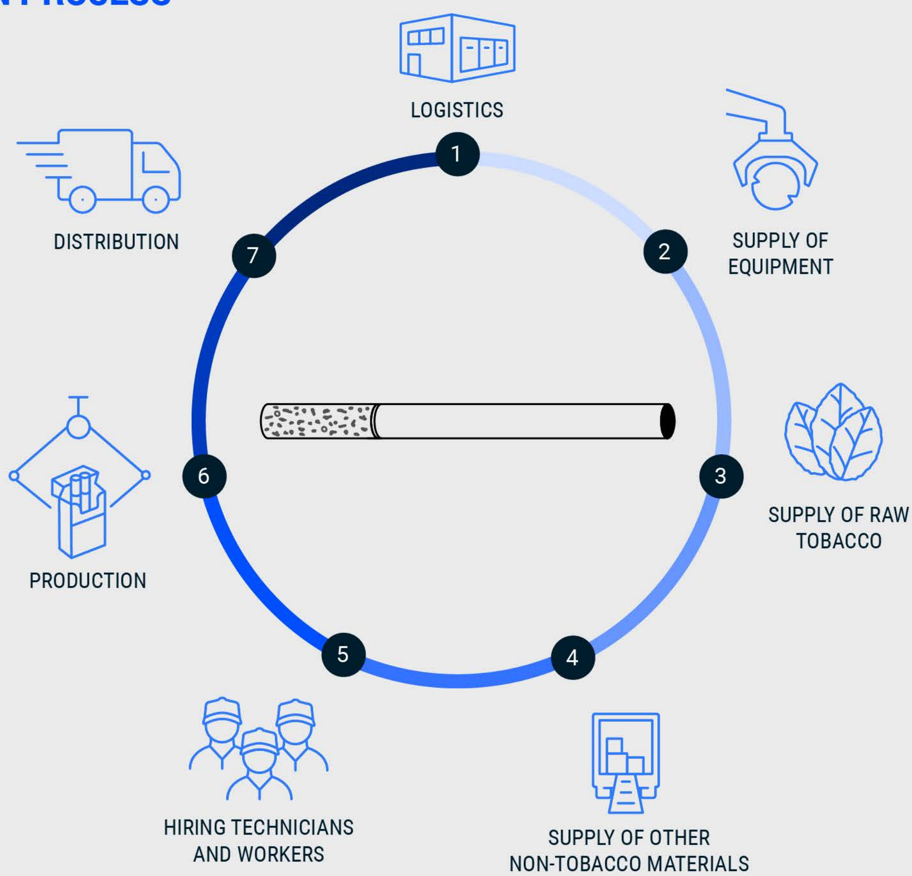
Smuggling and manufacturing illicit cigarettes brings high profits to organised criminal networks operating in the EU. The EU sets a minimum excise duty on cigarettes, however most Member States charge a much higher rate. All Member States also levy different rates of VAT on cigarettes. Legitimate tobacco prices have increased in many Member States but the demand for tobacco products has remained high, leading to a significant increase in counterfeit cigarette consumption in the last years. Criminal

[XIII] The Excise Movement and Control System (EMCS) monitors the movement of excise goods under duty suspension within the EU. It records, the movement between authorised consignors and consignees of alcohol, tobacco, and energy products for which excise duties have still to be paid. More than 100 000 economic operators currently use the system, and it is a crucial tool for information exchange and cooperation between Member States. The EU Commission has released the EMCS Mobile App (m-EMCS), intended for excise officers using the EMCS on the spot to monitor the movements of duty-suspended excise goods in the EU.

networks involved in the smuggling and production of illicit tobacco products operate with ample resources and adaptable modi operandi. Local facilitators also originate from the EU. These groups are highly resilient, as investigations often reveal the same involved actors. Hierarchically structured networks are predominant in large-scale tobacco smuggling and production. Criminal collaboration is common, with production, transportation, storage, distribution, and money laundering often carried out by cooperating networks.

Criminal networks are often involved in many other subsidiary criminal activities such as document fraud, tax evasion, the firearms trade, counterfeiting, cybercrime, trafficking in human beings, and property crime (theft of vehicles). Corruption is often used, taking the form of bribes to customs and police officers and port, cargo, and transport employees. Moreover, drug manufacturing sites have been discovered at the same locations of illicit tobacco factories. Criminal networks may be also involved in migrant smuggling, while labour exploitation has been identified at several illicit production sites where workers were forced to live on the premises and faced serious health risks.

THE BASIC STEPS OF THE ILLICIT CIGARETTE PRODUCTION PROCESS



Illicit production of counterfeit tobacco products

The illicit production of counterfeit tobacco products in the EU has grown, influenced by a combination of factors (such as the disruption of supply chains during both the pandemic and the Russian invasion of Ukraine, improved security in the trade of original branded cigarettes, and high and rising excise duties and taxes on tobacco products within the EU). Criminal networks are increasingly establishing illegal production sites in Europe, closer to the intended destination markets.

Large production facilities are usually located in industrial areas, on the outskirts of cities and near transportation hubs or haulage businesses, to disguise the movement of the trucks loaded with the illicit products. To avoid law enforcement detection, illicit factories often have autonomous power generators, closed-circuit television (CCTV) and other surveillance equipment, and soundproofing and insulation materials around doors and windows. A factory is typically active for two to three months before being dismantled and moved to a new location. Criminal networks increasingly use larger facilities and modern equipment to increase their production capacity. The original production markings are often removed from the equipment and machinery so they cannot be traced back to the supplier. Raw tobacco can be imported legally in leaf form, and the absence of a common regulatory framework makes it harder for law enforcement to monitor suspicious consignments.

On average, 12 to 14 workers operate a full production facility, which can produce 1 to 2 million cigarettes per day. Raided facilities included accommodation, sometimes built underground, where workers were housed. Professional criminal networks organise the various steps of the production process at different premises: sites for actual production of cigarettes, sites for cutting raw tobacco, and other sites for packaging and storage of precursors (raw tobacco, glue, filters, paper, etc.). In this way, if a cutting facility is identified by law enforcement, the rest of the production process is unaffected and cutting can be resumed somewhere else. This business model reduces risk and ensures the continuity of production.

Waterpipe tobacco is a type of combustible tobacco that is smoked with a waterpipe (also known as a hookah, maassel, shisha, narghile, or argileh). Waterpipe tobacco products are subject to excise duty like other tobacco products and they must comply with specific requirements. Recent seizures showed that the EU market for illegal waterpipe tobacco has grown over the last few years in response to increasing consumer demand in the EU. Illicit manufacturing is managed by criminal networks, in collaboration with other networks involved in smuggling of cigarettes but also non-tobacco materials. In some cases, companies are registered so as to enable import of precursors and to facilitate handling of criminal profits.

Smuggling of tobacco products from third countries takes several forms; criminal networks most often abuse the Excise Movement and Control System and the T1 procedure[XIV]. Criminals use trucks and vehicles to smuggle illicit tobacco products by road using cover loads and misdeclarations. They often infiltrate transport and shipping companies.

Fuel products

Fuel fraud is a growing phenomenon, with criminal networks involved in several types of fraud related to the production and trade of fuel. Fuel fraudsters exploit differences in legislation across EU Member States about the circulation of petroleum products and designer fuels (which are exempt from the Excise Movement and Control System). Fuel fraud is a complex criminal process typically carried out by individual criminals or groups that manage the entire supply chain and retail. Fuel launderers rely on the expertise of professionals, such as chemists and/or workers operating in the oil

[XIV] T1 is a transport for goods coming from outside the EU or not yet released into free circulation. These goods cannot be traded because import duties and VAT have to be paid first.

industry. In designer fuel fraud, specialised criminals use new additives and modify the physical characteristics of the final compound in order to avoid taxation.

Designer fuels – mixed mineral oils

Designer fuel is trafficked throughout the EU and causes huge revenue losses. Designer fuel is a mixture of gas oil and other components added to modify the physical characteristics of the final product. Criminal networks change the components and additives used in production, and transport gas oil under fake Combined Nomenclature codes to avoid the excise duty regime. The known illicit designer fuel production is lessening; the volume was 130 million kg in 2020, 160 million kg in 2021 and 77 million kg in 2022, due to the disruption of raw material (gas oil) supply from Russia combined with law enforcement measures. Attempts to circumvent EU sanctions may lead to fuel/oil smuggling. Criminals involved in the production of designer fuel operate internationally using missing traders and rely on the knowledge and expertise of professionals.

The emerging biofuel market

The emerging biofuel market might create opportunities for fuel launderers and fraudsters. Possible schemes could involve sale of biofuels that have not been sustainably produced and/or imported from third countries which do not comply with EU regulations. Such biofuels may be of suspicious origin and may be produced by oil blending[88].

Alcohol

The threat from alcohol excise fraud has been heavily mitigated due to the COVID-19 pandemic and the restrictive measures, which increased border controls but also closed relevant businesses such as restaurants and bars. Production continues to an extent, including overproduced and undeclared alcohol stemming from legitimate production sites operated by criminal actors.

During the pandemic, there was a high demand for disinfectants and the increased movement of ethyl alcohol, a non-excisable good with high alcohol content. Fraudsters watered down disinfectants, removed denaturants, and distilled them into spirits with an alcohol content of 40 %. After bottling and labelling, they sold these products as alcoholic drinks, without paying VAT or excise duty. Illegally transported alcohol was also sometimes disguised as disinfectants[89].

The restrictive trade sanctions in the framework of the Russian war of aggression against Ukraine made it more difficult to smuggle alcohol products such as vodka into the EU.

Customs import fraud

Customs import fraud consists of the evasion of duties on goods imported into the EU and involves the false declaration of the goods' value, their origin, and the classification that applies to them. Customs import fraud results in billions in financial losses[90], with damages for the economy and the financial interests of the EU, creating unfair competition and leading to market distortion. Document fraud is an essential component of this criminal activity. The most common modi operandi are:

- Undervaluation of goods on import declarations, often using fraudulent documents. The criminals, based on the agreement with the supplier of said goods, are declaring under-evaluated values for the commodities as a main method or by splitting the invoices in smaller ones, so that in the end the value of each individual invoice is lower. The undervaluation is always followed by national tax evasion or an intra community VAT fraud that relies on a network of missing traders, buffers and/or conduit companies.

- Misclassification of products imported into the EU, falsely declaring the category of goods according to the TARIC code[XV], in order to pay a lower duty rate.
- False declaration of the origin of goods to circumvent customs duties, including anti-dumping or countervailing[XVI] rules imposed by the EU on a particular country, producer, or on a product from a specific country.
- Dumping products on the EU market at a price lower than their normal value. The normal value is either the product's price as sold on the home market of the non-EU company, or a price based on the cost of production and profit.

Customs import fraud schemes are complex schemes that require extensive knowledge of customs procedures (CPs). Criminal networks involved in these fraud schemes are adaptive to the relevant regulatory amendments and able to exploit legislative gaps. CPs often reported to be abused by criminal networks are CP 40 00 and CP 42 00[XVII]. The abuse of CPs is often combined with VAT fraud (including carousel fraud).

China remains a main country of origin for goods imported into the EU with the use of customs fraud schemes[91]. Fraudulent schemes involving goods imported from China can combine several modi operandi, such as undervaluation, misuse of CP 42 00, and false declarations of final destination.

Criminal networks target fast moving consumer goods (FMCGs), such as sugar, textiles and shoes[92], and products that are high in demand in the EU (such as bikes and bike spare parts[93]), as well as intangible goods. Certain goods benefit from EU customs duties exemptions when they are imported from specific countries, and criminal networks exploit this regime by declaring a false country of origin. Cases of underdeclaration of the value of imported goods, as well as cases of false declarations of countries of origin, transit and destination, show the ability of criminal networks to exploit beneficial import procedures[94]. The special import procedures applying to imports from free trade zones (FTZs) are also exploited in customs fraud schemes, particularly in relation to the concealment of the origin of the goods[95]. The increase in the proportion of online retail and global shipping capacity has had an impact on customs import fraud[96], while the increased volume of small shipments using post and parcel services remains a key challenge. Customs import fraudsters are often also involved in VAT fraud (including carousel fraud), commodity counterfeiting, and money laundering. Complex patterns of shell companies established in many jurisdictions allow fraudsters to operate globally[97], and are used to justify the trade routes through fake importers or conduit companies[98].

[XV] TARIC stands for 'TARif Intégré Communautaire' (or Integrated Tariff of the European Communities). This 10-digit code indicates the customs tariffs and rules connected to import within the EU (Business.gov.nl, TARIC code.

[XVI] Countervailing Duty applies to goods that have benefited from government subsidies in their country of origin. Countervailing measures counteract the effects of subsidised imports on the EU market and restore fair competition.

[XVII] Customs Procedure 40 00 - Goods are released into free circulation following the payment of customs duty, VAT and other taxes (anti-dumping taxes, countervailing duties, agricultural taxes, excise duties and vehicle taxes). If the package undergoes import customs clearance in the territory of the destination country, all duties must be paid prior to the release of these goods into free circulation for the importer to be able to dispose of them freely. If the packages hold a preferential origin, they may be cleared under a reduced rate or zero rate. This means that customs duties do not have to be paid, only the VAT is charged on import. Fraud schemes abusing CP 40 00 occur when a fictitious preferential origin is declared on import. Another modus operandi is to misuse an indirect customs representative, which conducts the customs clearing procedure on behalf of the importer. After the products are imported in the EU they are usually moved to missing traders located in Member States which fail to account for and pay VAT.
Customs Procedure 42 00 - Customs Procedure 42 00 is a regime that allows importers to, under certain conditions, obtain a VAT import exemption when the imported goods are subsequently transported from the Member State of importation to another EU Member State. The VAT is due in the Member State of destination. Fraud schemes abusing CP 42 00 occur when the goods do not really end up in the Member State declared as final destination, but they are rather sold in the country where the import exemption has been obtained.

VAT fraud (including carousel fraud)

Value-added tax (VAT) fraud involves avoiding payment of VAT or fraudulently claiming repayments of VAT from national authorities. Within VAT fraud, carousel fraud or Missing Trader Intra-Community (MTIC) fraud is the most common criminal scheme in the EU. The prevalence of this crime has remained stable overall in the EU over the last two years. Reverse charge mechanisms[XVIII] introduced in some countries for commodities often targeted by fraudsters (i.e. mobile phones and electronics), have to some extent reduced the growth of the crime area.

Carousel fraud takes advantage of legislation which allows trading across Member States to be VAT free; VAT is only applied to sales within a Member State at the applicable domestic rate. Any VAT charged on sales should be declared and paid to the Member State's revenue authority. In cases of fraud, the first company in the chain charges VAT to a customer, but does not pay this to the government, becoming what is known as a 'missing trader'. Several billion euros are lost annually to carousel fraud schemes taking place in the EU[99], causing significant tax revenue losses.

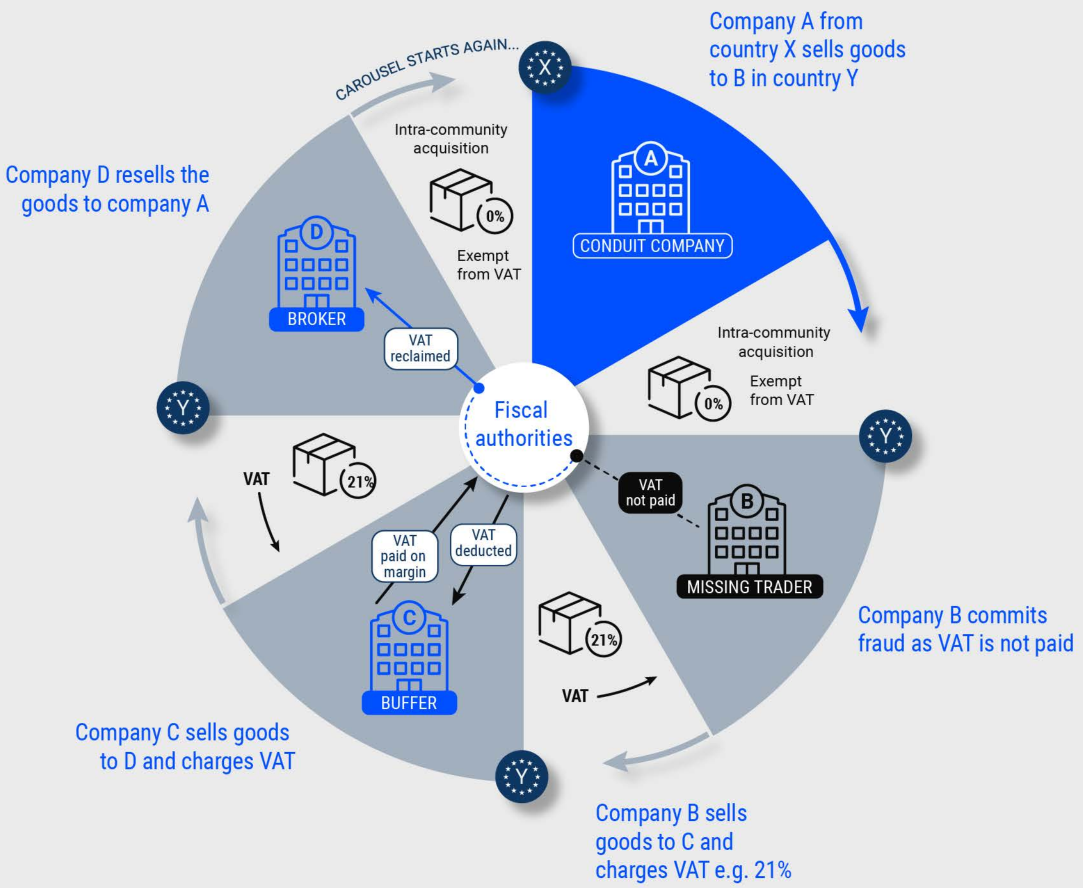
The ability of traders to go missing depends on the regulations regarding establishing, operating, and disbanding companies, and on VAT rules. Regulations vary across Member States, and in some cases there are few checks or requirements and companies are able to start operations without having shareholders - sometimes only registering an address remotely via national tax portals[100]. Countries applying high VAT rates on specific goods or services are more likely to be targeted by carousel fraudsters[101]. In more complex schemes, countermeasures are adopted to protect illicit profits from law enforcement detection, for instance using missing traders that do not receive any payment. Fraudsters also rely on logistics and transport companies, and in some cases exploit FTZs.

Carousel fraud involves the sale of goods or services from one trader to another, going round as in a carousel.

- Company A (conduit company) in Member State X sells goods or services to company B (missing trader) in Member State Y. Here the zero-rate VAT tariff applies.
- Company B sells the goods and services to Company C (broker company) in Member State Y, and here the VAT rate of Member State Y applies. Company B then disappears without paying the VAT amount to the government.
- Company C delivers the goods to D and charges VAT.
- Company D then sells the goods or services back to Company A in Member State X - a cross border sale between two Member States and therefore D charges 0 % VAT. As company D bought the products on the domestic market of Member State Y, it had to pay VAT to company C. The sell between Company D to company A in Member State X is an intra-community sell and therefore Company D can ask for a refund of the VAT paid to company C. Therefore, a double loss occurs for the budget of Member State Y as the missing trader (company B) never remits the VAT due and the broker (company D) requests for a refund of the VAT paid to the missing trader[102].

[XVIII] Where VAT is not charged by the supplier but accounted for by the customer (as taxable person) in his VAT return.

CAROUSEL FRAUD



Case example

A criminal network integrated a carousel fraud scheme into the regular commercial activity of an online company selling electronic devices, to avoid paying VAT. The network purchased SD cards with VAT from Dutch companies identified as missing traders, then sold them to companies in Croatia and Czechia with zero VAT, in accordance with intra-EU tax rules. Conduit companies based in Croatia and Poland were used to sell the VAT-exempt goods back to the missing traders in the Netherlands, and buffer companies were used to conceal the illicit transaction chain. The buffer companies purchased the SD cards from the missing traders and only paid VAT on a small margin made from the transactions. As is common practice in carousel fraud, payment for the transactions was made in advance[103].

Criminal actors and business model

VAT fraud is committed by professionals with extensive knowledge of the VAT system, legislation, and tax administration procedures. Criminal networks rely on experts in accounting, finance, tax, and technical knowledge (e.g. VoIP), as well as lawyers and other facilitators. They respond quickly to changes in legislation and the market, and also after law enforcement action. The geographical spread of VAT fraud is wide, and involves criminal networks made of different nationalities, most often EU nationals.

VAT fraudsters rely on the abuse of legal business structures. Criminals create complex networks of companies to conceal the actual connections between the scheme participants. Business entities hold several roles in the fraudulent schemes[104]:

- **Missing trader:** a VAT-registered trader who acquires goods or services without paying VAT, then supplies them with VAT, which he keeps rather than paying it to the tax authority.
- **Defaulter or default trader:** submits statements but fails to pay the VAT.
- **Buffer:** buffer companies are used to distance the broker from the missing trader. They usually buy goods or services from the missing trader and sell them to the broker with a small profit margin, on which they pay VAT.
- **Broker**: the broker claims and receives reimbursement for VAT payments that never occurred.
- **Conduit company:** at the start of a fraud scheme, the conduit sells goods or services across a border VAT-free to a missing trader in another Member State. At the end, the conduit acquires the goods or services back from the broker across the border; the transfer is VAT-free and the broker can claim the VAT that has been charged, but never paid by the missing trader.
- **Remote missing trader:** like a conduit company, a remote missing trader does not submit VAT statements. It is a company incorporated in a Member State other than the declared destination of the goods, used to mask the real destination.
- **Cross-invoicer:** buys commodities from another Member State with zero-rate VAT and sells them to a buffer company applying the domestic rate of VAT. To offset the output VAT, the cross-invoicer then declares acquisition from a national missing trader of goods or services that he subsequently delivers or exports to third countries.
- **Invoice mills:** companies that are set up solely to generate invoices that allow recovery of VAT, exploiting the practical impossibility of crosschecking every invoice against evidence that earlier tax has been paid.

Case example

In 2022, Operation Admiral uncovered the largest carousel fraud ever detected in the EU, establishing links between 9 000 businesses and over 600 individuals in different countries[105]. Criminal networks ran a complex carousel fraud scheme with electronic goods, causing an estimated tax revenue loss of EUR 2.2 billion. The criminal activities were perpetrated in almost all Member States and several non-EU countries, using a network of legal business structures. Some companies acted as legitimate suppliers of goods, and others claimed VAT reimbursements while selling the devices online to individual customers – and subsequently channelling the proceeds offshore before disappearing. Other companies laundered the criminal proceeds.

Criminal networks set up companies and make them disappear at the right moment[106]. Business entities with few or no employees and with no physical business premises are also used. Individuals in economic difficulties are often recruited to act as frontmen. In some cases, fraudsters take control of a legitimate business's VAT number and issue false invoices in their name. Companies on the brink of bankruptcy also appear in fraudulent schemes, declaring themselves bankrupt when tax authorities seek to retrieve VAT[107].

Non-traceable payment methods such as payment platforms are common[108] in VAT fraud. VAT fraudsters set up their own underground payment platforms and misuse existing banking and payment platforms, as well as online banking. Misdeclarations (misdescriptions of the origin and transit of the goods, or misclassifications for the goods to be classified with a lower duty rate and a lower VAT amount) are common with high-consumption food products and raw materials or semi-finished goods imported for processing within the EU.

Targeted commodities

Fraudsters target multiple tangible and intangible products and trade them over routes covering EU and non-EU countries.

Electronic products, particularly mobile phones and components, are among the most widely reported commodities. IT goods and accessories also appear in carousel frauds. Food products and beverages (including alcohol and spirits), are another common commodity, also due to the difficulties in following the flow of goods. High-demand food products and FMCGs, such as soft drinks and confectionery, as well as second hand cars, including luxury second hand cars[109], are often targeted. Precious metals, including gold, are an emerging commodity in VAT fraud schemes through misdeclaration[110]. The restriction of movement and economic slowdown caused by the COVID-19 pandemic had an impact on compliance activity and trading activities, and new commodities were targeted by criminals, such as personal protective equipment (PPE), FMCGs, and small electronics for remote working.

Carousel fraud schemes with intangible goods, such as VoIP primarily, but also advertising, marketing services, construction services, and counselling, continue to be reported in the EU. Intangible goods remain a threat in MTIC fraud and authorities increasingly face difficulties with trade in intangible goods, classified as 'services' for VAT purposes[111]. VoIP fraud is a developing area of VAT fraud within the EU[112]. A modus operandi in carousel fraud with VoIP is to use existing IMEI numbers not matching traded mobile phones or in combination with fictitious transports. It is complicated to detect and control the true source of such goods.

When intangible goods are traded between EU Member States, it is the responsibility of the purchaser to account for VAT in their domestic VAT statement. If the purchaser is a missing trader, a mismatch will be generated between the national VAT statements and the VAT Information Exchange System (VIES)[XIX]. However, if the purchaser is a cross-invoicer who submits the VAT statements, the criminal scheme will be harder to detect, as there are no mismatches with the VIES. In addition, imports and exports of intangible goods and services do not require any customs declarations. These features appeal to MTIC fraudsters, who integrate intangible goods and services into their established schemes. The energy sector also remains a target for criminal networks, including the trade in energy efficiency certificates (white certificates), CO_2 Emissions Trading System (ETS) certificates[113], and Guarantees of Origin for renewable energy.

Fraud schemes linked to sporting events

Match-fixing for betting-related and other reasons is a criminal activity enabled by corruption. Football remains the most targeted by international criminal networks in the EU, with a particular focus on sports actors in lower-level competitions and youth clubs[114]. Smaller leagues and competitions are more vulnerable as they lack resources to implement key countermeasures, and there is less media coverage. Other affected sports include basketball, tennis, handball, and cricket. Match fixers are likely to increasingly target the growing e-sports market, which offers very high prize money for teams and individual players.

Case example

In July 2023, in an operation supported by Europol, officers of the Spanish National Police have arrested 17 members of a criminal network engaged in sports corruption. Among the detainees are the president and players of a club playing in the fifth tier of the Spanish football league. The individuals are suspected of manipulating matches and placing large bets on their outcomes. The investigation, which is still ongoing, is focused on matches that were played on the final match day of the season, once the investigated team had been relegated. Upon receiving a large number of bets on specific results and noticing considerable amounts being gambled, bookmakers became suspicious and reported these findings[115].

Criminal actors in this area consist of both opportunistic individuals and criminal networks. Criminal networks use a wide network of connections to facilitate contacts with players, players' agents, and match and club officials in the EU and beyond. They target sporting events worldwide, sometimes multiple events that are happening at the same time, and the associated betting activities through online or offline providers. EU-based criminal networks often cooperate with collaborators in Asia to place bets. They mostly exploit Asia-based betting companies, but European betting operators are targeted as well. One criminal network can apparently orchestrate large match-fixing operations in several sports competitions across multiple countries.

Doping in sports is another way to influence the results of sports competitions by enhancing the performance of athletes using performance-enhancing drugs. Suspensions imposed by sports governing bodies and federations may last from a few years to life-long bans.

[XIX] The VIES (VAT Information Exchange System) is a search engine owned by the European Commission that allows to check if a business is registered to trade cross-border within the EU. The data is retrieved from national VAT databases when a search is made from the VIES tool.

INTELLECTUAL PROPERTY CRIME AND COUNTERFEITING

Criminal networks involved in intellectual property crime infiltrate every step of the legal supply chain, with a direct impact on public health and the safety of consumers. The crime area remains hard to investigate, as most of the counterfeited commodities traded within the EU originate from abroad, making the detection of the key players much harder. Furthermore, the digitalisation of trade and transport has shifted most of the distribution online, while offline sale has drastically reduced, further distancing criminals from their commodities.

Intellectual Property Crime (IPC) refers to criminal activities infringing intellectual property[XX] rights (IPR) such as copyrights, designs, geographical indications, patents, and trademarks. IPC affects many commodities (goods and services) and markets, from high-end consumer luxury goods to business-to-business products and common consumer products. Digital piracy affects diverse copyright-protected domains, including broadcasting channels, via Internet Protocol Television (IPTV), as well as audio-visual, literary and artistic content, etc.

- Most of the counterfeited commodities traded within the EU originate from abroad, making the detection of the key criminal actors much harder.
- The digitalisation of trade and transport has shifted most of the distribution of counterfeit goods online, further distancing criminals from their commodities. Distribution of counterfeit goods mainly occurs on the surface web.
- The detection of illicit laboratories importing product components and manufacturing the final products within the EU is increasing.

This crime area, including its modi operandi, criminal actors and geographical scope, has remained stable over the years, as it offers high-profits and low risks[116]. Detection of IPR-infringing goods dropped due to the COVID-19 pandemic[XXI], then recovered or increased in almost all EU Member States in 2021-2022[117]. The most commonly

[XX] Intellectual property refers to “creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce”, as defined by the World Intellectual Property Organization (WIPO).
[XXI] The number of seized articles had decreased by more than 13 % and their estimated value by almost 19 % from 2019 to 2020. EUIPO-European Commission (DG TAXUD), December 2021, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020. Accessible at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_EU_enforcement_intellectual_property_rights/2021_EU_enforcement_intellectual_property_rights%20_FullR_en.pdf

detained seized IPR-infringing goods are packaging material and labels, cigarettes, clothing, foodstuff and toys[118]. However, the key threats posed by IP crime in the EU relate to a broader spectrum of targeted sectors. The digitalisation of trade and transport has shifted most of the distribution of counterfeit goods online, while offline sale has drastically reduced. Distribution of counterfeit goods mainly occurs on the surface web via ad hoc websites, social media or online marketplaces. Online distribution puts further distance between criminals and their commodities.

The masterminds behind the trade in counterfeit goods in the EU are often located outside the EU and rely on intermediaries, either internal or outsourced, who ensure the running of the criminal process while providing the leadership with a shield to cover the upstream part of the chain.

Commodities and sectors most affected by IPC

The trade in counterfeit automotive spare parts is a rising threat in the EU, posing health, safety and environmental risks[119]. Several car brands reported a sharp increase[120]. Counterfeit airbags are a growing area of concern. Counterfeit spare parts are both manufactured and sold alongside genuine parts at legitimate businesses. Counterfeits are largely produced in Asia, but recent investigations highlight large production networks with advanced equipment operating within the EU.

Large quantities of counterfeit ready-to-use clothing and accessories are imported into the EU. There has also been an increase in imports of parts (e.g. branded fabric labels), destined for final assembly in the EU, which are ordered online and shipped by post or in luggage, often split into multiple shipments.

Detections of illicit laboratories of cosmetics and perfumes, which are importing product components and manufacturing the final products within the EU, have increased[121]. It is more common for assembly sites and clandestine workshops in the EU to apply counterfeit packaging and labels to unbranded ready-to-use products.

Although counterfeit foodstuffs seizures in the EU reportedly decreased in the past years[122], recent investigations reveal that criminal networks are using increasingly sophisticated production methods, targeting high-value products, such as luxury wines and spices.

Seizures of IPR-infringing packaging materials have continuously increased in recent years, both at the EU's external border and in the internal market, along with seizures of labels, tags and stickers[123]. In 2021, packaging materials became the most frequently encountered category of counterfeit articles seized across the EU, followed by labels, tags, and stickers[124]. China, including Hong Kong, and Vietnam to a lesser extent, have remained the main countries of origin in recent years[125]. Packaging materials, logos and labels are usually shipped separately from counterfeit goods. Deliveries are often split up over time or sent to different addresses, to limit the risk of customs seizures.

Pesticides are among the most highly regulated goods in the EU[126]. Illicit 'ready-to-use' pesticides and generic component products are imported in small parcel shipments to workshops located in Europe where they are converted into counterfeit pesticides[127]. Other modi operandi include relabelling seized stocks or banned and expired pesticides, blending or diluting products, and refilling original pesticide containers[128]. Use of blank bottles, sale after expiry, and use of the parallel trade system are also seen in the EU[129]. Criminals often forge documents and fail to apply warning labels for imported substances[130].

Some illicit pharmaceutical products are produced in EU-based illegal laboratories, which remain difficult to detect and require relatively few resources[131]. Distribution of diverted and stolen legit pharmaceutical products also occurs. Illicit hormonal substances are sometimes labelled as food supplements, making detection more challenging[132]. Illegal online pharmacies posing as legitimate vendors have surged over the last two years. Most of the illicit trade happens particularly through temporary websites, sometimes using targeted ads on social media or instant messaging applications.

Case example

In the 2022 edition of Operation SHIELD, French authorities targeted a criminal network trafficking psychotropic drugs (Pregabalin). The drugs were collected in legal pharmacies in Rhone-Alpes (France) using stolen and falsified medical prescriptions from doctors from all over the country. The criminal network was located in France with offshoots in Austria, Germany, and North Africa. Key members regularly travelled abroad to obtain the drugs (mainly in Belgium and the Netherlands). 20 individuals were arrested[133].

The modi operandi and the scale of piracy remains relatively stable. Growing demand for online entertainment during the COVID-19 pandemic led to an increase in distribution of illegal IPTV and illicit file sharing via peer-to-peer (P2P) networks using torrents or Direct Connect. However, improved access to legal platforms, and enforcement scrutiny in some EU Member States, led to a drop in users for these illicit platforms[134]. Piracy networks use new technologies to conceal digital traces and they use proxy services to increase resilience. The websites illegally distributing video content are hosted on servers across Europe, Asia and the Middle East, reducing costs. Much of the criminal profit is generated by online advertising, paid subscriptions, and malware attacks[135].

Case example

In May 2023, Europol has supported the Dutch Fiscal Information and Investigation Service (FIOD) in taking down an illegal Internet Protocol television (IPTV) service serving over 1 000 000 users across Europe. A series of raids were carried out across the Netherlands as part of an illegal streaming crackdown. Several individuals were arrested on suspicion of involvement in the illegal streaming of premium content. Packages bought by subscribers gave them access to over 10 000 live TV channels, alongside library of 15 000 films and TV shows[136].

Toys are among the most commonly seized illicit goods in the EU. However, the criminal networks involved, their modi operandi and their structure remain an intelligence gap, despite targeted major operations since 2020[137] which led to a significant increase in seizures.

Currency counterfeiting

Currency counterfeiting involves production and distribution of counterfeit currency, including reproduction of individual security features[138]. Counterfeiters in the EU produce counterfeit versions of euros and other local currencies in use by Member States outside the euro area[XXII]. The latter are typically produced and distributed at national and regional level. Some seizures in the EU have included counterfeit US dollars, British pounds and Russian rubles. Although in the last five years the number of counterfeit euro coins increased, the threat of this crime has diminished over the last two years in the EU as the COVID-19 pandemic led to an increase of cashless payments[139].

Criminal actors and criminal networks

Criminal networks involved in currency counterfeiting originate from both EU and non-EU countries[140]. Criminal networks active in this crime area show a high level of technical expertise and internal organisation, with different affiliates in charge of supplying equipment, production and printing, handling contact with potential markets and distribution, and as currency counterfeiters – the latter requiring more experience[141]. Criminal networks maintain secrecy among affiliates, for instance regarding the identity of the members in charge of printing. There are opportunity-driven connections between criminal networks, mainly for the supply of raw materials, and sometimes for the distribution to certain markets[142] across borders.

Case example

One criminal network is believed to have produced and distributed a total of more than three million counterfeit banknotes for a total face value of over EUR 233 million. This represents one quarter of all counterfeit euro banknotes detected in circulation since the introduction of the euro. The mastermind behind the scheme was involved in currency counterfeiting for more than 20 years. He established the whole counterfeit currency production network, and also organised dissemination on the European market. The investigation uncovered links to the Camorra group[143].

Production and distribution

Counterfeit euro banknotes distributed in the EU are primarily produced in various Member States of the EU. Raw materials, such as holograms, paper, and special inks, often come from Asia, purchased via e-commerce platforms and shipped in parcels and envelopes. Offset and digital printing remain major production methods for counterfeit banknotes. Illegal print shops are set up at various locations, including private premises and living spaces. Production methods and materials change depending on the type of counterfeit currency[144]. In some cases, criminal actors split the production and storage of counterfeits between different places and in smaller quantities, to minimise the risk of loss in case of arrest and seizures.

[XXII] These include the Hungarian forint (HUF), the Czech koruna (CZH), the Croatian kuna (HRK), the Romanian leu (RON), the Swedish krona (SEK), the Bulgarian lev (BGN), the Polish zloty (PLN) and the Danish krone (DKK).

EUROPOL RESPONSE

Europol is the EU's law enforcement agency and it assists the Member States in their fight against serious international crime and terrorism. Established in 2000, Europol is at the heart of the European security architecture and offers a unique range of services. Europol is a support centre for law enforcement operations, a hub for information on criminal activities, and a focal point for law enforcement expertise. Europol's operational architecture comprises five expert centres focusing on the different types of the serious and organised and terrorist crime spectrum:

- the Operational and Analysis Centre (OAC)
- the European Serious and Organised Crime Centre (ESOCC)
- the European Cybercrime Centre (EC3)
- the European Counterterrorism Centre (ECTC)
- the European Financial and Economic Crime Centre (EFECC)

The European Financial and Economic Crime Centre (EFECC) was established in June 2020, as Europol's answer to the growing threats posed to the economy and integrity of financial systems. These threats include money laundering, corruption, counterfeiting, fraud and tax fraud schemes that target individuals, businesses and public institutions. EFECC enhances Europol's operational and strategic support by preventing and combating financial and economic crime in the European Union. EFECC promotes the consistent use of financial investigations and asset forfeiture, while forging alliances with public and private entities. Financial and economic crimes are also tackled by EC3, such as in relation to complex cyber-enabled frauds. EFECC's role is to support the financial investigations of all other centres.

Europol's Financial Intelligence Public Private Partnership (EFIPPP) is the first transnational information sharing mechanism ever established in the field of anti-money laundering and counter-terrorist financing. Launched in 2017 as a joint project of Europol and the Institute of International Finance, EFIPPP provides an environment for cross-border cooperation and information exchange between Europol, competent authorities (including financial intelligence units and law enforcement agencies) and regulated financial service entities.

Europol closely cooperates with the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO) and the European Union Intellectual Property Office (EUIPO). OLAF's purpose is to investigate corruption and serious misconduct within EU institutions, as well as fraud against the EU's budget. EPPO is the EU's independent public prosecution office and is responsible for investigating, prosecuting and bringing to judgment the perpetrators of crimes affecting the financial interests of the EU. This pertains to crimes such as fraud, including cross-border VAT fraud with damages above EUR 10 million, money laundering of assets derived from defrauding the EU budget, and corruption and misappropriation affecting EU funds. The EPPO is also competent for offences regarding participation in a criminal organisation. The EUIPO is the agency of the EU responsible for managing the EU trademark and the registered Community design, European and international cooperation in the field of intellectual property, as well as the European Observatory on Infringements of Intellectual Property Rights.

CONCLUSIONS

Serious and organised crime is primarily driven by financial gain, and as such also drives the development of financial crimes. Corruption and money laundering are bridges between the licit and the illicit world, threatening to erode trust in authorities, in the rule of law and in the general functioning of society itself. The most lucrative criminal markets - such as drug trafficking, migrant smuggling, trafficking in human beings, excise and other types of fraud - generate billions of illicit proceeds on an annual basis. Virtually all these forms of serious and organised crime depend on money laundering to conceal the sources of illegally obtained funds, so that criminal networks can re-invest them and further expand their illicit undertakings.

Today, the limited degree of recovery of criminal assets indicates that criminal networks are successful in retaining and re-investing their illicit proceeds. An estimated EUR 4.1 billion of criminal assets were seized on average per year in 2020 and 2021 in EU Member States. This represents a two-fold increase compared to earlier estimates; however, it still stands for a small share of what criminal networks are believed to illicitly acquire in terms of financial gain. This shows that conducting parallel financial investigations is not a standard practice yet throughout EU law enforcement– even if this is a prerequisite for the recovery of more criminal assets and for better protecting citizens and the legal economy. The investment of billions of euros of laundered illegal profits in the licit economy distorts competition and the overall dynamics of a free market environment, ultimately hindering economic development. In parallel, the ability to retain criminally acquired funds, and reinvest them in criminal activities or services, presents a key threat to the internal security of the EU as it advances criminal structures and markets.

Criminal proceeds also fuel corruption, which in its turn furthers crime. Criminal networks infiltrate private or public entities in order to obtain information and facilitate money laundering through corruptive practices. Vast criminal proceeds available to many criminal networks make bribes a marginal cost and, therefore, a frequent practice. Corruption erodes the rule of law, weakens state institutions, and it is also detrimental to economic growth. In recent years, the reliance of serious and organised crime on corruption has become more visible and widespread. It occurs at all levels of society and targets any sector of importance - both in the private and the public realms. Criminal networks build networks of corrupted individuals in multiple organisations and hubs, from employees of private companies and public institutions, to politically exposed persons, law enforcement and justice personnel.

Victimisation as a result of financial and economic crimes, also including online fraud schemes and intellectual property crimes, is unprecedented and is likely underreported. Millions of victims are affected in the EU, also in large part due to the accelerated cyber-dimension of such crimes. Perpetrators are adept at exploiting the increasing online presence of EU citizens, businesses and public institutions alike. The impact of financial and economic crimes is enormous, not only financially, but also in terms of mental and physical health. With the phenomenon of re-victimisation, when the same victims are defrauded consecutively, the harm is even further amplified. Criminal actors' profits - and the associated losses of the private sector as one of the key target domains - are enormous, with single cases at times amounting to billions of euros in damage caused. Financial and economic crimes target the financial interests of the European Union and of the EU Member States, mainly via sophisticated VAT, customs and subsidy fraud schemes, thus hampering the overall economic stability and recovery in the Union.

Criminal actors involved in financial and economic crimes rely extensively on a wide range of professional experts that serve as essential enablers of their criminal activities. They demonstrate a high level of cooperation with professional service providers who can facilitate the infiltration of criminal profits into legal business structures, including the financial and real estate sector, or set up complex legal commercial entities for criminal purposes and for hiding ultimate beneficial owners.

Financial and economic crimes have an external dimension and as such are not limited to the EU only, but represent a problem of a global scale. The European Union, with its strong economy and high standard of living, is a prime target. Often, criminal operators from outside the EU take advantage of countries and jurisdictions with deficits in international anti-money laundering standards and in law enforcement cooperation. They are coordinating their criminal activities from such places, making strategic use of distance and communications technology in order to stay under the radar of law enforcement. From there, they target EU Member States, their citizens, and the overall stability of our public institutions. Such jurisdictions outside the EU inevitably pose a risk to the security and prosperity of the EU, an obstacle that can be effectively addressed only through truly global cooperation, including - but also beyond - the field of law enforcement.

In the next years, the consequences of the global multi-crisis context and further technological developments will continue to affect how criminal networks involved in financial and economic crime position themselves to pursue their interests. They are likely to continue to build on characteristics such as agility, inventiveness, cohesion, global reach, and financial power. Criminal activities will become even less confined to specific criminal structures and geographical bases of operation. Crime-as-a-service as the standard business model will bring criminal activities within the reach of more players in the criminal field, functioning as a multiplier for organised crime. In the long-term, the strengthening of anti-money laundering regulations will make it more difficult for criminals to legalise their criminal proceeds. As the opposite side of the coin, highly adaptive criminal networks will likely look for new tools and techniques to circumvent such strengthened frameworks. The role of financial and other experts may become even more important in this respect, assisting criminal networks in exploiting the continuous technical advances in the financial sector.

With the strengthened sanctions regime at the EU level in the context of the Russian war of aggression against Ukraine, enhanced cooperation among law enforcement authorities will be required in order to effectively address the “criminalisation” of violation of sanctions. The EU’s transition to a more environmentally sustainable and resilient economy aspires for a better future, but at the same time holds risks for criminal misappropriation. Different fraud schemes, corrupt practices, the misappropriation of funds, the criminal misuse of the growing environmental industry and the damaging side-effects of the counterfeiting of goods on the natural environment may hamper the ambition of this momentum of change. More sophisticated fraud schemes, targeting emerging markets in the green transition, are also to be expected.

As a global problem, in addition to cooperation with law enforcement partners within the EU, a multidisciplinary and comprehensive approach is required to tackle financial and economic crimes affecting the EU. Despite the strengthened legislative framework within the EU to address the threat posed by economic-financial crimes, financial investigations need to become a standard law enforcement practice when investigating serious and organised crimes. This will require substantial investment in resources and training.

METHODOLOGY AND DATA SOURCES

The report relies on an extensive analysis of data contributed to the Europol database, including information from investigations conducted in the framework of Operational Task Forces targeting high-value targets. Relevant strategic and operational reports produced during the reporting period complement the data collected and enhance the intelligence picture. Cases reported to Europol for operational reasons were also analysed to provide strategic insights.

Specific analytical questions and current intelligence gaps were addressed through strategic questionnaires on corruption, corruption in sports, money laundering, asset recovery, excise fraud, VAT fraud (including carousel fraud), commodity counterfeiting and intellectual property crime, and currency counterfeiting, as well as a separate data collection on online fraud schemes. A total of 300 responses to the strategic questionnaires were received. All relevant partners were consulted, including police, customs administrations, and other relevant actors such as tax authorities in the EU Member States, financial intelligence units and asset recovery offices, international networks for law enforcement cooperation (such as the Camden Asset Recovery Inter-Agency Network (CARIN)), relevant EU agencies, bodies and institutions, as well as the private sector via the Europol Financial Intelligence Public Private Partnership (EFIPPP). EMPACT members were involved in the data collection and were also invited to share operational and/or strategic information.

Reports from relevant EU bodies and agencies and reliable public-private partners, research studies, and open source information were taken into account to complement in-house information and to enrich the intelligence picture. Whenever data sources pointed to different directions, a qualitative assessment of the importance of the relevant indicators was carried out to help determine the relevant causal relationship.

The reference period for this report runs from July 2020 until the date of publication.

LIST OF ACRONYMS

AI	Artificial Intelligence
AMO	Asset Management Office
ARO	Asset Recovery Office
ATM	Automated Teller Machine
ATO	Account Takeover
BEC	Business Email Compromise
BNPL	Buy Now Pay Later
BTC	Bitcoin
CARIN	Camden Asset Recovery Inter-Agency Network
CCTV	Closed-circuit Television
CEO	Chief Executive Officer
CO_2	Carbon Dioxide
CP	Customs Procedure
DeFi	Decentralised Finance
EC3	European Cybercrime Centre
ECC	Elliptic-curve Cryptography
ECTC	European Counterterrorism Centre
EFECC	European Financial and Economic Crime Centre
EFIPPP	Europol's Financial Intelligence Public Private Partnership
EPPO	European Public Prosecutor's Office
ESOCC	European Serious and Organised Crime Centre
ETS	Emissions Trading System
EU	European Union
EUIPO	European Union Intellectual Property Office
EUR	Euro
FIOD	Fiscal Information and Investigation Service
FIU	Financial Investigation Unit
FMCG	Fast Moving Consumer Good
FTZ	Free Trade Zone
IBAN	International Bank Account Number
IP	Internet Protocol
IPC	Intellectual Property Crime
IPR	Intellectual Property Rights
IPTV	Internet Protocol Television
IT	Information Technology
IVTS	Informal Value Transfer System
LBS	Legal Business Structure
MTIC	Missing Trader Intra-Community
NFT	Non-fungible Token
NGEU	EU Next Generation Fund
OAC	Operational and Analysis Centre
OLAF	European Anti-Fraud Office

P2P	Peer-to-Peer
PPE	Personal Protective Equipment
PSD2	Payment Services EU Directive 2
SD	Secure Digital
TARIC	Integrated Tariff of the European Communities
TBML	Trade-based Money Laundering
UBO	Ultimate Beneficial Owner
US	United States
VAT	Value-added Tax
VIES	VAT Information Exchange System
VoIP	Voice over Internet Protocol

ENDNOTES

[1] Europol, 2017, Serious and Organised Crime Threat Assessment (SOCTA) 2017, accessible at https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017
[2] Europol press release, 23 January 2023, Bitzlato: senior management arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested
[3] European Commission, Directorate-General for Migration and Home Affairs, 2021, Mapping the risk of serious and organised crime infiltrating legitimate businesses : final report, accessible at https://data.europa.eu/doi/10.2837/64101
[4] SensorTower, 2022. European Adoption of Buy Now, Pay Later Apps Reached a Record 10 Million Installs in H1 2022, accessible at https://sensortower.com/blog/state-of-buy-now-pay-later-apps-europe-2022
[5] Information contributed to Europol
[6] Europol, 2021, Europol Spotlight – Cryptocurrencies: Tracing the evolution of criminal finances, accessible at https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances
[7] Chainalysis, 2022, The 2022 Crypto Crime Report, Original data and research into cryptocurrency-based crime, accessible at https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
[8] Europol, 2022, Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab, accessible at https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know
[9] Europol, 2023, European Union Terrorism Situation and Trend Report 2023 (TE-SAT), accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat
[10] European Council, May 2022, EU restrictive measures against Russia over Ukraine (since 2014), accessible at https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine
[11] Information contributed to Europol
[12] Information contributed to Europol
[13] Information contributed to Europol
[14] European Council, January 2023, EU sanctions against Russia explained, accessible at https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/
[15] Information contributed to Europol
[16] Europol press release, January 2023, Bitzlato: senior management arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested
[17] Europol, 2021, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[18] Ibid.
[19] FATF, Frequently Asked Questions, How is money laundered?, accessible at https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab
[20] FATF, July 2018, Professional Money Laundering, accessible at https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Professional-money-laundering.html
[21] Europol, 2021, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[22] Ibid.
[23] Ibid.
[24] Information contributed to Europol
[25] Information contributed to Europol
[26] Europol Press Release, 15 September 2022, One of Europe’s biggest money launderers arrested in Spain, accessible at https://www.europol.europa.eu/media-press/newsroom/news/one-of-europe%E2%80%99s-biggest-money-launderers-arrested-in-spain
[27] FATF, 2013, The role of Hawala and other similar service providers in money laundering and terrorism financing, accessible at https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf
[28] Information contributed to Europol
[29] European Commission, Directorate-General for Migration and Home Affairs, 2021, Mapping the risk of serious and organised crime infiltrating legitimate businesses : final report, accessible at https://data.europa.eu/doi/10.2837/64101
[30] Information contributed to Europol
[31] Information contributed to Europol
[32] Europol, Money Muling, accessible at https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/money-muling
[33] Information contributed to Europol

[34] Chainanalysis, 2022, The 2022 Crypto Crime Report, Original data and research into cryptocurrency-based crime, accessible at https://go.chainalysis.com/2022-Crypto-Crime-Report.html
[35] Financial Intelligence Unit – Nederland, 9 February 2021, De over het paard getilde handelaar, accessible at https://www.fiu-nederland.nl/knowledge_base/de-over-het-paard-getilde-handelaar/
[36] World Customs Organisation, June 2022, Illicit Trade report 2021, accessible at https://www.wcoomd.org/en/media/newsroom/2022/june/the-wco-issues-its-2021-illicit-trade-report.aspx
[37] Europol, December 2022, Seizing the opportunity: five recommendations for crypto assets-related crime and money laundering, accessible at https://www.europol.europa.eu/publications-events/publications/seizing-opportunity-five-recommendations-for-crypto-assets-related-crime-and-money-laundering#downloads
[38] Europol, January 2022, Cryptocurrencies: tracing the evolution of criminal finances, accessible at https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances
[39] Ibid.
[40] Information contributed to Europol
[41] Ibid.
[42] Europol, 2021, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[43] European Commission, Directorate-General for Migration and Home Affairs, 2021, Mapping the risk of serious and organised crime infiltrating legitimate businesses : final report, accessible at https://data.europa.eu/doi/10.2837/64101
[44] Europol, 2022, Europol Spotlight, Shadow money - the international networks of illicit finance, accessible at https://www.europol.europa.eu/publications-events/publications/shadow-money-international-networks-of-illicit-finance
[45] Information contributed to Europol
[46] FATF, 2019, Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs), accessible at www.fatf-gafi.org/publications/documents/rba-trust-company-serviceproviders.html
[47] Information contributed to Europol
[48] Europol, 2022, Europol Spotlight, Shadow money - the international networks of illicit finance, accessible at https://www.europol.europa.eu/publications-events/publications/shadow-money-international-networks-of-illicit-finance
[49] Information contributed to Europol
[50] Europol, 2021, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[51] UNODC, 2004, United Nations Convention against Transnational Organized Crime and the Protocols Thereto, article 2(f), accessible at https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
[52] European Commission, Confiscation and freezing of assets, accessible at https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/confiscation-and-freezing-assets_en
[53] European Commission, May 2022, Directive of the European Parliament and the Council on asset recovery and confiscation, COM(2022) 245 final, accessible at https://ec.europa.eu/home-affairs/proposal-directive-asset-recovery-and-confiscation_en
[54] Europol, 2016, Does crime still pay? Criminal asset recovery in the EU, Survey of statistical information 2010-2014, accessible at https://www.europol.europa.eu/publications-events/publications/does-crime-still-pay;
[55] Information contributed to Europol. It needs to be noted that the 2016 estimate was based on statistical information of 21 out of then 28 EU Member States.
[56] RAND Europe, 2019, Understanding the revenues earned on criminal markets and their reinvestment in the EU legal economy, accessible at https://www.rand.org/randeurope/research/projects/economic-value-of-illicit-markets-european-union.html
[57] Europol press release, 27 June 2023, Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized, accessible at https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized
[58] Europol, 2021, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[59] Ibid.
[60] Information contributed to Europol
[61] Corruptie.org, What is corruption, accessible at http://www.corruptie.org/en/corruption/what-is-corruption
[62] Information contributed to Europol
[63] Information contributed to Europol
[64] Europol and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam, 2023, Criminal networks in EU ports. Risks and challenges for law enforcement, accessible at https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement
[65] Information contributed to Europol

[66] Europol, 2021, Europol Spotlight, Shadow money, the international networks of illicit finance, accessible at https://www.europol.europa.eu/publications-events/publications/shadow-money-international-networks-of-illicit-finance
[67] Europol and OLAF, 2022, Assessing the Threats to the NextGenerationEU (NGEU) fund, accessible at https://www.europol.europa.eu/publications-events/publications/joint-europol-olaf-report-assessing-threats-to-next-generation-eu-ngeu-fund
[68] Information contributed to Europol
[69] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[70] Europol 2021, Internet Organised Crime Threat Assessment, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
[71] Information contributed to Europol
[72] Information contributed to Europol
[73] Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, accessible at https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[74] Europol, 2022, The Europol Podcast – Targeting scam call centres, accessible at https://www.europol.europa.eu/media-press/europol-podcast/episode-7-targeting-scam-call-centres
[75] Information contributed to Europol
[76] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[77] J. Yang, J. Gunzberg, M. Good, B. Keoun, CoinDesk, December 2022, CoinDesk Market Outlook: 4Q Crypto Gloom Spills Into 2023, accessible at https://www.coindesk.com/consensus-magazine/2022/12/20/2023-crypto-price-market-outlook/
[78] Europol press release, 24 June 2021, Europol helps Belgian and Swiss authorities unravel Vitae Ponzi scheme, accessible at https://www.europol.europa.eu/media-press/newsroom/news/europol-helps-belgian-and-swiss-authorities-unravel-vitae-ponzi-scheme
[79] Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, accessible at https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[80] Europol and EUIPO, 2021, Misleading invoice fraud targeting the owners of intellectual property rights, Crime situation in 2021, accessible at https://www.europol.europa.eu/publications-events/publications/misleading-invoice-fraud-targeting-owners-of-intellectual-property-rights-crime-situation-2021
[81] Chainalysis, 2022, Crypto Crime Report 2022, accessible at https://go.chainalysis.com/2022-Crypto-Crime-Report.html
[82] Information contributed to Europol
[83] Europol press release, 11 August 2021, Unmasked: 23 charged over COVID-19 business email compromise fraud, accessible at https://www.europol.europa.eu/media-press/newsroom/news/unmasked-23-charged-over-covid-19-business-email-compromise-fraud
[84] Europol press release, 8 April 2021, Beware of scams involving fake correspondence from Europol, accessible at https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol
[85] Europol press release, 14 July 2023, 27 food fraudsters arrested in Lithuania and Italy, accessible at https://www.europol.europa.eu/media-press/newsroom/news/27-food-fraudsters-arrested-in-lithuania-and-italy
[86] Europol press release, 15 October 2021, New operation to protect Next Generation EU recovery funds, accessible at https://www.europol.europa.eu/media-press/newsroom/news/new-operation-to-protect-next-generation-eu-recovery-funds
[87] Europol press release, 23 June 2021, Six arrested for siphoning €12 million in fraudulent COVID-19 unemployment payments from France, available at https://www.europol.europa.eu/media-press/newsroom/news/six-arrested-for-siphoning-%E2%82%AC12-million-in-fraudulent-covid-19-unemployment-payments-france
[88] Information contributed to Europol
[89] Information contributed to Europol
[90] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[91] OLAF, 2021, The OLAF Report 2020, accessible at https://anti-fraud.ec.europa.eu/document/download/73e011db-693b-4b87-9e8a-5858cc3c2d_en?filename=olaf_report_2020_en.pdf and OLAF, 2022, The OLAF Report 2021, accessible at https://anti-fraud.ec.europa.eu/about-us/reports/annual-olaf-reports_en#modal
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Europol, 2021, EU Serious and Organised Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/publications-events/main-reports/socta-report
[96] Ibid.
[97] OLAF, 2022, The OLAF Report 2021, accessible at https://anti-fraud.ec.europa.eu/about-us/reports/annual-olaf-reports_en#modal
[98] Ibid.

[99] Europol, June 2020, Enterprising criminals, Europe's fight against the global networks of financial and economic crime, accessible at https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime
[100] European Parliament, Policy Department for Budgetary Affairs Directorate-General for Internal Policies PE 731.902 - June 2022, Possible Solutions for Missing Trader Intra-Community Fraud, accessible at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/731902/IPOL_STU(2022)731902_EN.pdf
[101] Europol, June 2020, Enterprising criminals, Europe's fight against the global networks of financial and economic crime, accessible at https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime
[102] European Parliament, Missing Trader Intra-Community Fraud, accessible at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690462/IPOL_BRI(2021)690462_EN.pdf
[103] Europol press release, 12 February 2021, VAT fraud clampdown: international scam with memory cards uncovered in the Netherlands, accessible at https://www.europol.europa.eu/media-press/newsroom/news/vat-fraud-clampdown-international-scam-memory-cards-uncovered-in-netherlands
[104] Europol, 2021, EU Serious and Organised Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/publications-events/main-reports/socta-report
[105] Europol press release, 13 December 2022, Europol support to EPPO investigation into EUR 2.2 billion VAT fraud scheme, accessible at https://www.europol.europa.eu/media-press/newsroom/news/europol-support-to-eppo-investigation-eur-22-billion-vat-fraud-scheme
[106] European Parliament, Policy Department for Budgetary Affairs Directorate-General for Internal Policies PE 731.902 - June 2022, Possible Solutions for Missing Trader Intra-Community Fraud, accessible at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/731902/IPOL_STU(2022)731902_EN.pdf
[107] Ibid.
[108] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[109] EPPO, 23 November 2022, Spain: EPPO probes into VAT fraud in luxury car sales with estimated losses of €12 million, accessible at https://www.eppo.europa.eu/en/news/spain-eppo-probes-vat-fraud-luxury-car-sales-estimated-losses-eu12-million
[110] Information contributed to Europol
[111] European Parliament, Policy Department for Budgetary Affairs Directorate-General for Internal Policies PE 731.902 - June 2022, Possible Solutions for Missing Trader Intra-Community Fraud, accessible at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/731902/IPOL_STU(2022)731902_EN.pdf
[112] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[113] European Parliament, Policy Department for Budgetary Affairs Directorate-General for Internal Policies PE 731.902 - June 2022, Possible Solutions for Missing Trader Intra-Community Fraud, accessible at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/731902/IPOL_STU(2022)731902_EN.pdf
[114] Europol, 2020, The involvement of organised crime groups in sports corruption. Situation report, accessible at https://www.europol.europa.eu/publications-events/publications/involvement-of-organised-crime-groups-in-sports-corruption
[115] Europol Press Release, 27 July 2023, Odds were against 17 football match fixers, accessible at https://www.europol.europa.eu/media-press/newsroom/news/odds-were-against-17-football-match-fixers
[116] EUIPO-European Commission (DG TAXUD), December 2022, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020. Accessible at https://euipo.europa.eu/ohimportal/en/web/observatory/-/eu-enforcement-of-ip-rights-a-joint-report-with-the-european-commission
[117] Quantitatively assessed upon the EUIPO-European Commission (DG TAXUD), 16 December 2022, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020, accessible at https://euipo.europa.eu/ohimportal/en/web/observatory/-/eu-enforcement-of-ip-rights-a-joint-report-with-the-european-commission
[118] Ibid.
[119] OECD-EUIPO, March 2022, Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, Illicit Trade, OECD Publishing, accessible at https://doi.org/10.1787/117e352b-en
[120] Drive, 10 August 2022, Mercedes-Benz seized 1.8 million counterfeit parts globally in 2021, accessible at https://www.drive.com.au/news/mercedes-benz-counterfeit-parts-seized-2021/
[121] EUIPO and Europol, 2022, Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022
[122] EUIPO-European Commission (DG TAXUD), 16 December 2022, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020, accessible at https://euipo.europa.eu/ohimportal/en/web/observatory/-/eu-enforcement-of-ip-rights-a-joint-report-with-the-european-commission
[123] EUIPO and Europol, 2022, Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022; EU Commission and EUIPO, December 2022, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2021, accessible at https://taxation-customs.ec.europa.eu/news/eu-enforcement-ip-rights-joint-report-european-commission-2022-12-16_en

[124] EU Commission and EUIPO, December 2022, EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2021, accessible at https://taxation-customs.ec.europa.eu/news/eu-enforcement-ip-rights-joint-report-european-commission-2022-12-16_en
[125] Ibid.
[126] EUIPO and Europol, 2022, Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022
[127] Ibid.
[128] UNEP and GRID-Arendal, 2020, The Illegal Trade in Chemicals, accessible at https://www.unep.org/resources/assessment/illegal-trade-chemicals.
[129] EUIPO and Europol, 2022, Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022
[130] Ibid.
[131] Ibid.
[132] Ibid.
[133] Europol press release, 29 September 2022, Medicine traffickers faced with undesirable side effects, accessible at https://www.europol.europa.eu/media-press/newsroom/news/medicine-traffickers-faced-undesirable-side-effects
[134] EUIPO and Europol, 2022, Intellectual Property Crime Threat Assessment 2022, accessible at https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022
[135] Ibid.
[136] Europol press release, 23 May 2023, One of Europe's biggest pirate IPTV services taken down in the Netherlands, accessible at https://www.europol.europa.eu/media-press/newsroom/news/one-of-europes-biggest-pirate-iptv-service-taken-down-in-netherlands
[137] Europol, March 2022, Operation LUDUS I targeting counterfeit and other illicit toys, accessible at https://www.europol.europa.eu/publications-events/publications/operation-ludus-i-analysis-report
[138] Europol, 2021, European Serious and Organised Crime Threat Assessment (EU SOCTA) 2021, accessible at https://www.europol.europa.eu/socta-report
[139] Ibid.
[140] Europol press release, 3 July 2020, Counterfeit currencies worth millions of euros prevented from entering the EU economy in Romania and Spain, available at https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-currencies-worth-millions-of-euros-prevented-entering-eu-economy-in-romania-and-spain; Europol press release, 11 March 2022, 14 arrests for euro counterfeiting in Spain, accessible at https://www.europol.europa.eu/media-press/newsroom/news/14-arrests-for-euro-counterfeiting-in-spain
[141] Europol press release, 17 July 2020, Possibly largest ever bust of banknote counterfeiters in the history of the euro, accessible at https://www.europol.europa.eu/media-press/newsroom/news/possibly-largest-ever-bust-of-banknote-counterfeiters-in-history-of-euro
[142] Ibid.
[143] Ibid.
[144] Europol press release, 28 January 2021, Half a million in fake euros seized in Romania, accessible at https://www.europol.europa.eu/media-press/newsroom/news/half-million-in-fake-euros-seized-in-romania

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports